Operating Agreement
on the usage of IT equipment

between

the works council and the management
of the Helmholtz-Zentrum Berlin

§ 1 Area of application

This operating agreement applies to all employees as defined by §5 Absatz 1 BetrVG.

1. The operating agreement
    a. Applies to the use of electronic facilities and devices with the scope of information technology and their accessories, to the software installed hereupon, as well as to the IT network components in the HZB and to the services which connect the HZB to the science network and the Internet. Herein after all this will collectively be referred to as "HZB-IT".
    b. Applies to all employees and users of the HZB-IT at the Helmholtz-Zentrum Berlin (in the following referred to as "HZB-User").
    c. Regulates the general[1] handling of HZB-IT and communication networks and licenses.
    d. Does not regulate the handling of test-systems.
    e. Does not encompass the use of eduroam and the separately provided guest-WLAN.
    f. Does not govern the handling of scientific IT systems which are not part of the network of the HZB. Also this agreement does not govern the archiving of scientific data in the sense of good scientific practice.
2. Exceptions to this regulation need to be applied for with the central IT department.

§ 2 General terms of utilization

1. The general terms of utilization arise from the particular demands on the HZB as an operator of large research facilities with in-house research.
2. The HZB-IT has to be deployed in a cost-saving and resource-friendly manner. The principle of mutual consideration has to be followed. Any use of the HZB-IT must not obstruct the HZB's business operations.
3. The HZB-IT User are obliged to use the HZB-IT appropriately and carefully and to avoid damage. Any losses, disturbances, damages or faults have to be reported immediately to the Servicedesk (help@...).
4. Standard clients are made available for personal use to HZB-users by the central IT department. Prerequisite for this is a suitable order using the e.biss-procurement system. The specifications of standards for PCs, netbooks and mobile phones are documented in the intranet and will be adapted cyclically. Orders of work-place technology which diverge from these standards need a comprehensible justification from which is evident, why the offered standard technology is not suitable for the envisaged tasks, and need a special approval by HA-IT.
5. Installed protective measures have to be maintained (such as virus protection, Firewalls, etc.).
6. The operation of unauthorized WLAN´s or the creation of measures for external access to the HZB

[1]The word "basic" describes an in general approved and obliging rule which contains a special reservation. This exception is regulated is necessary separately.

network, as well as the inclusion of external devices is generally forbidden.
7. Special caution is advised when using external memory media (DVD, USB-Stick etc.). Special attention is required not to jeopardize the internal HZB-IT. This is applies in particular to the transfer of data from external media.
8. Users on business trips to destinations abroad have to inform themselves about the legal situation and risks abroad and have to take measures adequate to the risks involved, in order to safeguard the protection of information technology and data belonging to HZB. The IT department consults on preventive measures.
9. All applicable licensing terms have to be observed.

§ 3 Authorization of utilization

1. HZB-IT-users obtain their right to use the HZB-IT through an application for the granting of an authorization of utilization for the HZB-network or parts thereof.
2. An authorization of utilization can be granted to other people, provided they can substantiate a legitimate interest and provided that such an authorization does not pose any security risks.
3. The department IT-DS (information technology services and software) registers all authorized persons and maintains a suitable HZB-IT user-directory.
4. The authorization of utilization is strictly personal and is not transferable. It is forbidden to pass on authorizations and/or passwords to third parties or to make use of others. The HZB-IT-user is responsible for all activities carried under his/her user-id.
5. The application for a right of utilization has to be directed to the head of the department of IT-IS, using of the relevant application form and with the help of the user's secretariat.
6. The departmental head of IT-DS decides on the application.
7. If IT-DS rejects the application, the course of action has to be presented to the management for a final review.
8. IT-DS has to be informed immediately upon retirement of an employees by his/her organizational unit, in order to revoke access to the HZB-network and in order to reutilize HZB-property (hardware, software) is supplied to a wide use. The superior of the retiring employee is responsible for the return of the data to the HZB.

§ 4 Proper conduct of technology at the workplace

1. Depending on their intended use, personal computers have to be switched off at the end of the working day and during longer absence.
2. The screen has to be locked when leaving the workspace.
3. The use of private hardware with connection with the HZB-IT is prohibited.
4. Mobile devices owned by the HZB like phones (also smartphones), tablets or notebooks are to be kept safe and protected against unauthorized access. The HZB-IT-User is responsible that no other people obtain access to the device and that the device is protected against theft at all times.
5. SIM cards issued for business matters are not intended for use in private phones or similar equipment. Such use is prohibited.
6. Security features in use for mobile devices, like PINs, gestures or similar have to be treated and kept safe like passwords.

7. All incidents linked to malicious software have to be reported to the Helpdesk and the IT-security officer.

§ 5 Handling of data, data protection

1. HZB-IT-Users may process data they do with the consent of the owner of the data only.
2. The unauthorized transfer of data to third parties is forbidden.
3. Documents a HZB-IT-User is accountable for must be clearly marked as such and in a way that is unmistakable for others.
4. In order to prevent the abuse of data with special data-protection requirements, suitable measures have to be put in place by authorized HZB-IT-Users as well as the IT department. For the rest existing data protection and data backup procedures have to be used.
5. HZB-IT-User is obliged to follow regulations on representative participation and data-protection when processing or storing personal data.
6. Confidential or secret company data as well as personal data may be stored locally on mobile technology only, if no third party could access the data even upon loss of the mobile device.
7. When decommissioning data carriers, their data has to be deleted and the data carriers have to be destroyed professionally. Special data-protection containers for discarded data-carriers have been put in place at different locations at the WCRC in Adlershof and LMC in Wannsee. (see https://www.helmholtz-berlin.de/hzbin/dscon_list.pl)

§ 6 Net services

1. The “HZB-net” as defined by this operating agreement comprises the wired computer network of the HZB as well as the employee-WLAN on both sites. It does not encompass eduroam and the guest-WLAN, for which separate regulations apply.
2. Every HZB-IT-User can use Internet services like file transfer, e-mail, participation in discussion forums and WWW. He/she is advised to use these service only for his/her scientific, technical or official duties. In particular any commercial use is not permitted.
3. Regulations set out in “Richtlinien für HZB-Seiten im World Wide Web” are authoritative for the creation and design of web pages.
4. Access to the HZB-net may not be provided directly or indirectly to persons which do not have a user-id for the use of the HZB-IT.
5. When using the HZB-net the user is subject to restrictions which are given by law (e.g., data protection act), employment contract or valid internal regulations of the HZB.
6. Downloads liable to license agreements and/or liable to pay costs are permitted only within the scope of existing contracts.
7. Punishable, politically indecent, power-glorifying, immoral, pornographic, racist or inciting representations in picture, tone and writing are prohibited. The same applies to actions which violate applicable property rights and related rights (e.g., copyright, competition regulations, etc.). This is also valid for the use of social media in the net.

§ 7 Use of software and licenses

1. The main IT department provides the HZB-IT-User with suitable applications via a software-portal in the intranet.
2. The installation of private software on IT equipment belonging to the HZB is forbidden.
3. Copying HZB-owned software for private or commercial use is forbidden.
4. Software for official use has to be procured by the purchasing department.
5. Applications requiring a license to run may only be installed properly licensed.
6. The unauthorized transfer of licenses is prohibited.
7. Any official requirement to use software which has been classified according to $202c StGB as a so-called hacker-tool must be notified to the main IT department and approval has to be obtained from the IT-SiBe.
8. Before use or deployment of Open Source software the license terms have to be checked for restrictions and implications. The result of this investigation has to be communicated to IT-FH, stating the exact name of the software, the intended use, place of installation and the licensing terms.

§ 8 Use of special software

1. E-Mail
    a. The HZB provides every HZB-IT-User with a mail account on a central mail server operated by the IT and for the official work purposes.
    b. Official e-mails containing information which is subject to data-protection regulations may not be forwarded to private mail accounts.
    c. E-mails containing information which fall under data protection regulations must be encrypted even for HZB-internal transmission. To this end an application to obtain and use a personal certificate must be made with the certification authority of the HZB. (See https://www.helmholtz-berlin.de/zentrum/infra/it/dienste/ca/index_de.html)
    d. The folder “deleted elements” has to be emptied regularly.
    e. A signature will be added automatically to all mail with an external recipient address:

> Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
>
> Mitglied der Hermann von Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V.
>
> Aufsichtsrat: Vorsitzender XXX, stv. Vorsitzende XXX
> Geschäftsführung: XXX, XXX
>
> Sitz Berlin, AG Charlottenburg, 89 HRB 5583
>
> Postadresse:
> Hahn-Meitner-Platz 1
> D-14109 Berlin
>
> http://www.helmholtz-berlin.de

f. Thus, your own signature should only contain your function or job-title and phone number(s) (see pattern)

[Title] first Name surname

Function or Place name

[Institute]

Official tel.:

[Official Mobil number]

g. An automated notification of absence should be activated in the mail account, in particular if no automatic forwarding of mails is enabled during the absence.

2. Calendar:
   a. The central calendar is being operated for HZB-IT-users on the central Exchange-server.
   b. For groups, in addition to the central calendar a web-based calendar can be used too.
   c. HZB-IT-users using approved nonstandard client systems for their office communication are obliged to install an adequate mail program and are obliged to maintain their central calendar on their own. Appropriate software is being made available for users of standard client systems.

§ 9 Competence for surveillance and monitoring

1. The capacity to operate the HZB-net and central services lies with the main IT department.
2. The department IT-IS takes care of balancing the load on the HZB net. To this end IT-IS may limit network usage in order to maintain data protection, technical-operational procedures or for reasons of economical efficiency.

§ 10 Sanctions

1. Upon reasonable suspicion of an offence against this operating agreement the head of the IT-DS department or an authorized representative is allowed to inspect user-files, provided confidentiality is maintained at all times. Prior condition is the approval by the management-board on an individual basis. The works committee, the data protection representative and the IT-SiBe have to be consulted. The HZB user has to be informed without delay and stating the reason for the inspection. The inspection has to be recorded in writing and the result has to be presented to the management-board and to the user. The works committee needs to be consulted in case of activities pertaining to aspects concerning labor legislation.
2. In case of serious offences against this operating agreement the management-board may order a temporary or permanent exclusion, or a restriction of the use of the HZB-net or external network services. IT and A-PS will be notified about this. IT will immediately initiate suitable technical measures.

§ 11 Implementation

This operating agreement will come into effect on the 01.01.2017.