Directive on the use of Information Technology[1)]

Table of Contents

1) Please note that the present English language version serves solely for information purposes, in case of doubt or deviations only the original German language version is decisive.

Introduction

The Helmholtz-Zentrum Dresden - Rossendorf (HZDR) provides its employees and guests with the information technology infrastructure (IT infrastructure) of the HZDR, the workplace information technology and, if applicable, mobile IT devices for the fulfillment of their official tasks

A widely available, efficient, innovative and secure IT infrastructure is the key to effective work at the research center as well as for the provision and use of modern IT services. To ensure such effectiveness, certain rules must be observed by staff as well as by guests and visitors when working with these IT facilities. Adhering particularly to regulations concerning data security, data protection, access control and securely connected data devices is therefore of great importance for every individual user.

The department of Information Services and Computing (FWC) is responsible for organizing the IT infrastructure and the data and communication network. Information technology users (employees, business partners, guests and visitors) are obligated to adhere to the user conditions set forth in this regulation. Important additions to these operational regulations are contained in the Operational Agreement L121, which covers tele-media services at the HZDR.

1 Definitions, Scope and Terms of Use

1.1 Definitions

Regarding individuals at the HZDR, the following ***person groups*** are differentiated in HZDR-Regulation D 411:

- **Employees** (including trainees, assistants, doctoral candidates)
- **Business Partners**
- **Guests Scientists**
- **Visitors**
- **Others**

With respect to the IT use, individuals are differentiated between:

- **Guest users** (individuals without their own user account and with limited usage rights)
- **Users** (individuals with full usage rights)
- **Administrators** (persons with extended permissions)

Administrators are persons authorized by the FWC Central IT Department. There are central administrators (employees of FWC) and institute administrators, appointed by the heads of the institutes and central departments. The tasks and rights of the administrators are defined in L 221: "Regulations for the operation of information technology systems at the HZDR".

In this regulation, a distinction is made between the following device types with access to the data network:

- **Stationary Devices** (e. g. PC, printers, meters, IP phones, BMS)
- **Mobile computers** (including notebook, convertible)
- **Mobile smart devices** (smartphones or tablets, mostly with Android or iOS system)

This may be official equipment (property of the HZDR) or private equipment (property of the user or a contractor). They are also differentiated in terms of their ***configuration*** in:

- **HDZR-compliant devices**: A business IT device procured by the HZDR and configured by a responsible administrator in accordance with the HZDR guidelines. The guidelines for a compliant configuration (operating system, permissions, virus protection) are listed on the HZDR intranet.
- **Non-HZDR compliant devices**: Private or corporate IT device without HZDR-compliant configuration (e. g. measuring computer).

HZDR data network: The data and communication network of the HZDR comprises both wired and wireless networks (wireless LANs) and covers the Dresden-Rossendorf location and its research locations. The network is structured into different subnetworks for the different application areas and authorizations. There are internal networks (for example for IT services), separate networks for guests, infrastructural components (e.g. telephones, access control, building management systems) and also separate networks for certain research facilities (so-called "measurement networks").

The responsibility for the operation of the specific monitoring networks and of devices within those networks is often the responsibility of the administrator in charge. The gateways that provide access to these special networks are usually configured and operated by central IT.

1.2 Scope

The organizational, technical and infrastructural measures and methods described in this directive concerning IT usage are mandatory for all staff and guests at each HZDR location and also apply to all external users of the HZDR IT infrastructure. The regulations specified here apply to the acquisition, installation, operation and use of IT services, IT technology and software.

1.3 Terms of Use

Use of the HZDR IT infrastructure is permitted only with granted authorization after registration, the EDUROAM Wireless LAN can be used without registration. The user obtains an user account, permissions and information for accessing HZDR IT services from the Department FWC.

As well as other regulations, the user must agree to the following in order utilize the HZDR IT infrastructure:

- To utilize resources conscientiously and according to operational guidelines
- To not modify the hardware installation and to not alter the basic configuration of the operating systems or network without express consent of the central IT or the responsible administrator
- To not install or use any unknown, unregistered or improperly licensed hardware or software
- To strictly adhere to IT security and data protection regulations
- To refrain from any misuse of the IT systems and from attacks on authenticity, integrity and data privacy as well as to support all measures for observing and establishing IT security

By acquiring an official user account, the user acknowledges and accepts all provisions set forth in this HZDR-regulation (L111).

1.4 Authorizations

Central administrators are supported by administrators in the individual institutes and central departments. Administrative duties are carried out by the designated IT administrators. In exceptional cases (e.g., if software requires permissions or for operation or for certain mobile devices), local administration rights can be given to users who are competent and have been instructed in proper use.

To manage local administrative tasks, such instructed users will be provided a separate account with administrative rights if necessary. Assigning administrative rights to a personal user account is not permitted. An account with administrative rights may only be utilized for installing and configuring systems. The personal user account is to be used for standard workflows.

The user can look up the name of his/her responsible administrator on the Intranet:

https://www.hzdr.de/mydata

Further regulations concerning administrative responsibilities are set forth in L221: “Responsibilities and Functions of the Department of Information Services and Local Administrators”.

1.5 Using Guest Accounts

Special non-personalized user accounts are individually delegated to a HZDR administrator who is responsible for assigning the account and instructing the user on conditions of use. The passwords are to be regularly changed and guest accounts are to be deactivated when not in use.

1.6 Regulations on Leaving

At the end of staff employment, and/or at the termination of the contractual relationship involving guests or business partners, the authorization of use expires and the user accounts are automatically disabled. Upon justified request by the responsible supervisor or contact person of the HZDR the user can continue to use certain services (e. g. access his/her e-mail account) for a limited period of time if desired (generally three months, maximum one year).

Personal data will be deleted after this period, unless a renewed professional relationship is foreseeable within one year of departure. The storage of technical / professional data is to be clarified before departure with the responsible supervisor. Data connected to publications must be permanently archived at the HZDR (see A 213 Publications Directive).

1.7 Exclusion from Use

Infringements of the IT Usage Directive are punishable by the HZDR. Violations presenting imminent risk will result in immediate exclusion from IT system use.

Conscious violation or unauthorized use of the HZDR IT systems that damages HZDR interests or its public reputation, compromises the security of the network or breaches legal regulations, can lead to professional and/or other legal consequences.

2 Acquiring and Installing IT Components

2.1 Acquiring Hardware and Software

The HZDR is oriented on standard systems. The Department of Information Services and Computing determines the standard configuration after consultation with the IT Commission. The configuration will be adjusted at certain intervals, taking user needs and technical development into consideration. The standard systems are subject to competitive bidding and are made available by selected suppliers.

Deviations from the standard configuration can only be accepted for justified special requirements, such as with computers integrated into equipment or monitoring networks. Acquisition requests that deviate from the standard configurations require justification from the orderer (in the purchase order) with approval by the FWC.

The Department of Information Services and Computing (FWC) coordinates software acquisition. All software is registered in the HZDR software database through the acquisition process. The standard software for workplace computers is installed during initial configuration. The list of current standard software is coordinated with the IT Commission.

Results (data, projects, etc.) created with academically licensed software may not be used for commercial purposes (such as third party funded projects). This applies et al. for CAD programs, but also for modeling or programming systems. For this purpose, in part special commercial software licenses are used.

The use of software generally requires verification of the eligibility and availability of the necessary license by the user or his supervisor. By using the software, the user automatically agrees to accept the terms of the license. It is not permitted to illegally duplicate or distribute licensed software or to unlawfully use licensed software. The installation of application software may only be performed by an administrator if the user or his supervisor can prove that the user is authorized to use the software and has the corresponding license.

2.2 Installation Responsibility

The IT infrastructure of the HZDR is structured according to the requirements on the one hand and the technical boundary conditions on the other. Users must guarantee administrators access to the IT systems to an appropriate extent. Their measures to install and secure smooth operation are to be accepted - as far as permissible under data protection law. Such measures are, for example:

- Registration of hardware and software in the appropriate databases
- Installation and cabling
- Installation, updating and removal of hardware and software
- Setting and removing authorizations for users
- Analysis, logging and monitoring (within the framework of data protection law, see also company agreement L121).

3 Operation and Use of IT Systems

3.1 Use of IT Services of the HZDR

Each employee is provided with a personal HZDR e-mail inbox. The e-mail address usually consists of the first letter of the first name, the surname and the ending @hzdr.de (for example m.mustermann@hzdr.de). The change of the e-mail address can be made on request and with a corresponding justification.

For official communication only the HZDR e-mail address should be used. Service and external mailboxes must be kept strictly separate from each other. When accessing external mailboxes, it is preferable to use web access. In particular, users may not redirect official messages to an external mailbox or private messages to the office mailbox.

Business e-mails must be provided with a text signature at the end of the message. In terms of content and design, this essentially corresponds to the official business cards of the HZDR supplemented by information on the association. Formatting should be done in simple text, and the street address is optional. An authoritative sample is provided below:

Max Mustermann
Institute for Fluid Dynamics
Helmholtz-Zentrum Dresden - Rossendorf e.V.
Tel.: +49 (0) 351 260 1234
http://www.hzdr.de
Board of Directors: Prof. Dr. Sebastian M. Schmidt, Dr. Diana Stiller
Registration Court: VR 1693 at the District Court Dresden

In addition the e-mail must be signed with a digital HZDR certificate. This ensuresthe authenticity of the sender and the content of the message. All employees can request a personal digital certificate via the Intranet.

Further details and mandatory regulations on e-mail use can be found in L121: “Works committee agreement on the use of Tele-media Services at the HZDR” and on the Intranet under the following link: https://www.hzdr.de/e-mail

Each user will be provided with access to storage and computing resources of the HZDR for official purposes. It is not permitted to store or back up official data on external cloud services (e. g. iCloud, GoogleDrive); HZDR's own web-based cloud services must be used for this purpose. This also applies in particular to the login data for the services of the HZDR.

3.2 Connection of IT components

Active data network components (switches, routers, WLAN access points, converters, etc.) may only be installed and modified by employees of the FWC data network group or have to be approved by them. The connection of modems at locations of the HZDR is prohibited, in justified cases a spe-cial permission can be granted. Changes to the data network cabling may only be carried out by the responsible FWC staff or authorized persons. Programs and devices for the management of the data network may only be used by the data network group or only with the permission of employees of this group.

The network connection of user devices is based on specific rules that ensure security and stable operation. In general, the connection of all IT devices to the data network requires registration via the HZDR procedures. Users who participate in the "eduroam" service at HZDR or at their host institutions can use the Internet access with their "eduroam" identification via the "eduroam" network without registering their devices.

HZDR devices must be registered and managed in the HZDR databases. FWC assigns the initial configuration parameters for the network connection (computer name, IP address, network configuration) for the device to be connected. The use of other configuration parameters must be coordinated with FWC and depends on institution-specific requirements. However, these must not conflict with already globally used parameters. Unregistered, improperly configured or network-disturbing devices will be excluded from use of the data network after consultation with the institute administrator.

Only HZDR-compliant IT devices (see 1.1) are allowed in the internal HZDR network. Guest networks are provided for ***non-HZDR compliant IT devices*** that allow the user to access limited network services (e. g. Internet access) after registering (the device or via "eduroam").

Subject to certain conditions, the registration of third-party devices for the internal network can be applied for (see https://www.hzdr.de/network). With the integration of "external devices", the owner / user submits to the regulations that apply at HZDR.

3.3 Use of stationary and mobile computers

The use of business computers provided by the HZDR is intended to perform work-related tasks. The installation of applications is done by an administrator, usually based on standard configurations. The Central Department FWC reserves the right to check the installed applications at regular intervals by means of log stitches.

Business mobile computers (notebooks) are essentially treated as stationary computers. Business notebooks that are used as workstations in the internal network regularly receive security settings and updates. As with stationary workstations, e-mail, contacts and calendars can be retrieved from the HZDR's e-mail servers via the native e-mail applications, or web services can be used as an alternative.

Compliance with IT security and data protection regulations (see Chapter 4) is of particular importance for mobile use. To protect sensitive data, those must generally be stored encrypted on mobile computers (see 4.5). Please also note the provisions of D 213 "General Works Agreement on Working Time and Mobile Working".

3.4 Use of mobile smart devices

Mobile smart devices provided by the HZDR, such as smartphones or tablets, have to be configured by the central department FWC before the first commissioning. Among other things, this configuration includes the inclusion of the device in the central mobile device management of the HZDR and the installation of a container app (e. g. "Sophos Secure e-mail"). This app can be downloaded from the corresponding app stores. Changes to this configuration are prohibited. The FWC Central Department reserves the right to check the units for deviating configurations at regular intervals.

The retrieval of e-mails, contacts and calendars from the HZDR servers must only be performed on mobile smart devices via the container app provided FWC or the HZDR's web services.

The use of social media applications on HZDR business devices is possible for of official tasks. It is generally important to ensure that no HZDR business data is passed on to third parties. This is ensured by the use of the HZDR container, but must be taken into account when configuring and using any other application.

3.5 Private Use

The Internet access is available to employees as working tool within the framework of task fulfillment and further training. Private use is regulated in L 121: "Works Agreement on the Use of Tele-media Services at HZDR".

The private use of the HZDR IT infrastructure is only permitted to a minor extent if the performance of the duties and the availability of the IT system for official purposes are not impaired and budgetary principles do not oppose this.

Private data, which is not required in the context of official task fulfillment, is not stored on local service computers nor on HZDR network or cloud storage. To ensure the availability of storage space for all users, the FWC Central Department reserves the right to delete such data after consultation with the user.

Private devices can be used to access HZDR services or data subject to certain terms of use. In this case, official and private data must remain strictly separate. The use of the web offers of the HZDR to retrieve the e-mails, calendars, contacts and released data via web browser is possible at any time. Furthermore, private mobile computers and smart devices can be used in the HZDR's guest networks.

As a rule, private devices may not be used for the synchronization and storage of business data. If a use is indispensable in individual cases, the synchronization of business e-mails, calendars and contacts is only permitted if this is done via an encrypted application (a HZDR-approved app). The use of such an app may result in specific data (system information, telephone number) being stored on HZDR servers.

3.6 External access to the data network and IT services

To access HZDR resources and data from outside via the Internet, various accesses (Citrix, SSH, HZDRCloud, ThinLinc, HIFIS services etc.) are available via gateways. Access is controlled by central firewalls. Multi-factor authentication is required to access critical resources from outside. The additional factor is configured in the user account and provided via a personal smartphone (https://www.hzdr.de/mfa).

All employees have access to web portals from where central services (https://www.hzdr.de/citrix) and central data (https://vpn.hzdr.de) can be reached. In exceptional cases, Virtual Private Network (VPN) can be used to directly access devices and services from external sources. This is to be requested separately. The authorization is granted to HZDR employees and, in exceptional cases, to guests as required. The access takes place via encrypted channels.

In addition to the necessary authorization, access to the HZDR network also requires a minimum level of security at the remote site (including up-to-date virus protection). When using private devices for dial-in, each user is responsible for securing the device accordingly. For the use of the services via external access, the same safety regulations and terms of use apply as for internal use at the HZDR and its research sites. The HZDR assumes no liability for any consequences that may arise from the use of this access to external devices.

For the use of approved mobile work, official equipment may be provided or, alternatively, private devices may be used. The designated compliant office computers automatically connect to the HZDR network, preferably a virtual workstation is opened at HZDR servers. Private devices used for mobile work are subject to the restrictions already mentioned for the synchronization and storage of official data, including e-mails. Again, the connection with a virtual workplace at HZDR or the use of the offered Web and Citrix services are the preferred usage options.

4 IT-Security and Privacy

4.1 Responsibility

IT security requires responsible and adept actions on the part of each individual user. Adhering to IT security within the given organizational security framework is the responsibility of each and every employee as well as the respective supervisors.

Central organization of IT security is overseen by the HZDR IT safety representative in cooperation with the Department of Information Services and Computing FWC and the data protection representative.

Unauthorized listening, recording or modification of data from the network as well as scanning the data network is prohibited. Remote access by administrators during active user sessions at a desktop computer or server is generally only permitted when explicitly activated by the individual user (see also 4.6).

Violations or interruptions that impact IT security or the protection and integrity of data are to be immediately reported to the IT security representative or the data protection representative.

4.2 Access Protection and Password Handling

Access to the IT systems is to be secured by staff from unauthorized use (switching off the device, logging off, password protection, etc.). All data devices (especially laptops, tablets, mobile telephones, etc.) are to be protected from unauthorized access and theft. Loss of such devices must be reported immediately.

Passwords are used exclusively for personal authentication and use. They are to be kept secret, meaning they may not be communicated to any other individual or revealed or stored in any manner.

Passwords are to be chosen by the user in such a way that they cannot be easily guessed by any other party (no obvious names or terms or combinations, and they must contain at least one special character). Passwords must conform to certain rules and are to be changed at regular intervals. The Department of Information Services and Computing FWC outlines these rules and monitors compliance. HZDR password guidelines can be found on the Intranet here: https://www.hzdr.de/passwd

4.3 Data Security and Protection

Die Zentralabteilung FWC stellt Dienste zur Ablage und Sicherung von Daten (Backup und Archivierung) bereit. Wichtige Daten sind auf den dafür zur Verfügung stehenden institutsinternen oder zentralen File-Servern abzulegen. Für die Speicherung dienstlicher Daten sind interne Angebote sowie ggf. Ressourcen der Kooperationspartner im Rahmen der Kooperationsvereinbarungen zu nutzen.

Nur auf den institutsinternen sowie zentralen Verzeichnissen und Servern erfolgt eine automatische Sicherung. Für die Sicherung und Archivierung lokal abgelegter Daten trägt jeder/jede Nutzer*in selbst die Verantwortung, er/sie kann dafür geeignete Werkzeuge nutzen, die ihm/ihr dafür bereitgestellt werden. Die Zentralabteilung FWC stellt zur Datensicherung geeignete Backupdienste bereit, die für einen Zeitraum von 90 Tagen mit inkrementellen Backups die darin erfassten Daten zur Wiederherstellung vorhalten.

Die Entscheidung über die Schutzwürdigkeit der Daten – und damit den Speicherort - obliegt dem pflichtgemäßen Ermessen der jeweiligen Verantwortlichen, sofern keine anderen Festlegungen getroffen sind. Die Übertragung und die Speicherung schutzwürdiger Daten (vor allem auf mobilen Geräten und Datenträgern) sollen verschlüsselt erfolgen. Datenträger mit schutzwürdigen Daten sind generell verschlossen aufzubewahren. Der Umgang mit personenbezogenen oder personenbeziehbaren Daten hat nach den jeweils geltenden Vorschriften des Datenschutzes zu erfolgen und ist mit dem/der Datenschutzbeauftragten des HZDR abzustimmen (siehe A 200 HZDR Anweisung zum Datenschutz).

Datenträger, die nicht mehr genutzt werden (Festplatten, Magnetbänder, CD‘ s, USB-Sticks u. ä.) müssen vor der Verschrottung bzw. der entsprechenden Geräte ausgebaut und fachgerecht gelöscht werden. Dies gilt auch für Datenträger bzw. Geräte mit Datenträgern welche an anderer Stelle weiterverwendet werden sollen. Unterstützt wird dies durch die Zentralabteilung FWC und die zuständigen Instituts-Administrator*inne The Department of Information Services and Computing FWC provides services for storing and se-curing data (backup and archiving). Important data is to be stored on the central file servers, made available for this purpose. For storing business data, internal options are to be utilized as well as resources provided by cooperation partners if needed.

Backup is only carried out on central directories and servers. Every user is responsible for backing up and archiving locally stored data. He can utilize appropriate tools provided for this task. FWC provides backup services that provide data for recovery for up to 90 days using incremental backups.

The decision on the legitimacy of the data - and thus the storage location - is the duty of the respective responsible parties, unless otherwise specified. The transmission and storage of sensitive data (especially on mobile devices and data carriers) should be encrypted. Data mediums with data worthy of protection should generally be kept locked. Dealing with personal data must be carried out in accordance with the applicable data protection regulations and must be coordinated with the data protection officer of the HZDR (see A 200 HZDR Instructions on Data Protection).

Data media that are no longer used (hard disks, magnetic tapes, CD's, USB sticks, etc.) must be removed from the corresponding device before scrapping those and then professionally deleted. This also applies to data carriers or devices with data media that are reused elsewhere. This is supported by the FWC central department and the responsible administrators.

4.4 Virus Protection, Spam and Web Filtering

The Department of Information Services and Computing FWC organizes the IT Thread protection at the HZDR. Each user must agree to take necessary precautions, and the centrally available virus scanners must be used on local computers. These scanners are automatically activated on Windows systems after initial installation. Virus protection is available for Windows, Linux and Mac operating systems, and installation is generally mandatory. For devices on which virus protection would severely limit use, suitable compensation measures are to be determined together with FWC. If infections or malfunctions are suspected, the Department of Information Services and Computing FWC must immediately be notified and the device must promptly be disconnected from the network. Devices lacking up-to-date virus protection are not permitted on internal networks.

To reduce potential threat to IT systems, the use of official removable media (USB sticks, external hard drives, etc.) is only permitted for official purposes. The data drives must be checked using an up-to-date virus scanner before use with an HZDR computer. Data downloaded from the Internet is automatically checked with a virus scanner and is moved into quarantine should an infection be detected. Use of personal removable media on HZDR devices is not permitted.

A central spam filter is utilized at the HZDR. According to the Works Agreement L121, suspicious e-mail is marked, and e-mail clearly identified as spam is blocked. A notification is not sent to the employee if a message is blocked. If a user suspects that an e-mail was falsely classified as spam, he/she should notify the department FWC.

A significant portion of malware is distributed by means of websites. The HZDR utilizes a web filter to warn users of harmful sites or sites with suspicious content and to block the content if necessary. Incorrectly classified sites can be reported at any time and will be unblocked. Web filter use is carried out as per the regulations set forth in Works Committee Agreement L121 and in agreement with the Works Council, the data protection supervisor and the HZDR management.

IT security regulations can be found on the Intranet here: https://www.hzdr.de/it-security

4.5 Encryption

To avoid loss of sensitive data through mobile device theft, such business devices are to be encrypt-ed (e. g., laptops, tablets, smart-phones). This is mandatory for all devices that leave the HZDR locations (if technically possible for that device).

For devices with Windows and macOS operating systems, the FWC Department provides a central mandatory solution for managing the encrypted information. For Linux devices, the operating system's internal encryption is to be used. The FWC supports setting up and managing these devices, but the responsibility for encrypting the equipment lies with the users and administrators. FWC can conduct random checks in regard to enforcing this regulation.

Files with increased need for protection are to be separately encrypted at the file level. The User Helpdesk and the IT security representative can provide assistance for setting up and implementing such encryption.

Further encryption regulations can be found on the Intranet here: https://www.hzdr.de/encryption

4.6 Virus Protection, Spam and Web Filtering

Bei der Nutzung von Fernwartungssoftware muss das gleiche Sicherheitsniveau erreicht werden, In using remote maintenance software, the same security standards must be observed as when utilizing internal services. Before utilizing remote maintenance software, the operators must be pro-vided instruction by the administrator. Only permissions and information that are absolutely neces-sary should be granted or released.

The institute utilizing the remote maintenance software in cooperation with the external company if applicable (e.g. for service issues) must ensure that this software is not misused and is only utilized in compliance with license conditions.

The remote maintenance software must not be connected permanently and must not be automated. It must always be actively started by the respective user. Remote maintenance procedures are to be supervised during all use.

Further regulations for utilizing remote maintenance software can be found under the following link: https://www.hzdr.de/remote-management

4.7 Using Messaging Services

By default, the centrally provided conference systems (e.g., video conferencing, chat) or HZDR options for the workplace are to be used (see information provided on the Intranet). If such use is not possible (e.g., due to demands by cooperation partners), local alternatives can be utilized. These must be coordinated with the IT security representative and are to be configured and to be kept updated by administrators. Users are not permitted to operate messaging servers.

Devices with internal microphones or cameras are to be removed from the room during confidential discussions or at least be switched off. A communication or messaging connection remains active once it is started until it is explicitly disconnected, even if the employee leaves the vicinity of the equipment. The connection is therefore to be terminated when leaving the equipment.

Further regulations on use of messaging systems at the desk can be found in the Works Agreement L121 covering “Use of Tele-media services at the HZDR” and in HZDR Directive L131 on "Social Media Policy."

5 Taking Effect

This HZDR Directive comes into force when signed and replaces all previous regulations on the subject.

Appendix

Services and Contacts

The first contact in case of problems in the workplace is always in charge of the respective institution / the corporate department administrator (see sec. 3.2). For the submission of support or problems questions there is a so-called "user helpdesk" in the HZDR Intranet:

- https://www.hzdr.de/support

This forwards the messages immediately and automatically to the competent administrators. There is also a telephone hotline:

- Hotline in the data center: +49 351 260 3317

Using the following link you can reach all relevant contacts and information:

- https://www.hzdr.de/FWC

Information and Links

The data center is located in building 614 and is open from 08:00 to 16:00. In this period, the hotline can be reached, the user registration is done and it you can send print jobs to be picked up.

All important information and interactive services, are shown in the intranet pages of the central IT Department FWC. Among other things, this link guides you to required applications:

- https://www.hzdr.de/itservices

For important messages about current maintenances or outages, see:

- https://www.hzdr.de/servicestates