Guidelines for data protection and IT security

Table of contents

Guidelines for data protection and IT security

1 Introduction

This guideline is to regulate the behavior of employees of the Medical University of Graz (Med Uni Graz) at the use of information and communication technology in the professional context of the Med Uni Graz as well as handling personal data. The basis for this are legal provisions such as, in particular, the data protection EU General Data Protection Regulation (GDPR), Austrian data protection law and the data protection adaptation laws as well as generally accepted IT data security standards or state of technology.

Against this background, the aim of this guideline is to protect, all personal data as well as business and trade secrets, but also and by means of the available information and communication technology (IKT), in such a way that only

- authorized access and allowed publications (protective aim: confidentiality)
- authorized modifications (protective aim: integrity) and
- authorized cancellations or interruptions (protective aim: availability) are possible.

In addition, the awareness of employees in the sectors data protection and IT security should be supported. The use of own hardware ("bring your own device") and the private use of IKT infrastructure will also be regulated.

2 IT Organization

2.1 Organizational Unit Information Technology

The organizational unit information technology (O-IT) operates, along with other internal organizational units, the IT systems at the Med Uni Graz. An efficient user service, centrally controlled data protection measures, the possibility of storing data on central file servers as well as the possibility of the implementation of programs on application servers are essential requirements for a safe and seamless IT use to support daily work processes.

The O-IT offers centralized services (e.g. operation of a server, monitoring services etc.).

The O-IT further on operates a service desk which can be reached by phone or e-mail. Contact info is available on the website of the O-IT.

The O-IT continuously sets measures for ensuring data protection (see **Appendix 2**).

The offered services of the O-IT for employees and students are available on the intranet.

2.2 IT Partners

IT partners are contact persons in the individual organizational units with basic IT knowledge, who act as contact persons for the O-IT and the employees. They deliver information to employees, provide onsite support, collect demands from the organizational units, and coordinate these with the O-IT.

The IT partners of the Med Uni Graz are of primary importance, as they have to initiate, coordinate and maintain records in their field of competence the, for the IT use offered, technical and organizational measures for data security. In case of questions about IT use they are contact persons for employees in their area as well as for third parties (e.g. WLAN-accounts for guests, information for guest lecturers).

3 Policies for Use of IT Infrastructure

3.1 Acquisition

The acquisition of soft- and hardware is carried out in accordance with instructions from the acquisition workflow with the O-IT of the Med Uni Graz. The acquisition of soft- and hardware at the university hospital Graz within the patient care is implemented by requirement forms, which are sent to the staff position for medical technology and the IT from the KAGes and transmitted from there to the O-IT. The installing of this software is implemented by the hospital IT, which is responsible for the compliance of standards and safety requirements.

Standard software such as MS Office, Corel and more are available free of charge for employees. Other products such as software by Adobe are offered at campus prices and are available through the acquisition workflow. Standard software is saved on the Q-drive of the Med Uni Graz and can be installed individually or jointly with the IT partners.

With in-house development of software, the professional and technical requirements and framework conditions for the operation of the software must be previously specified. These tasks will be carried out in accordance with the impacted areas, the O-IT is, in any case, to be calledin.

3.2 Password Policy

All IT systems and applications must be so arranged that only authorized users, with an authorized user recognition and password, have the possibility to work with them. Exceptions are possible in justified cases but are to be discussed with and set up by the O-IT. The allocation of usernames for the work on IT systems is generally personalized implemented. The work under the identification of another person is inadmissible. Users are forbidden to transmit identification codes and passwords to colleagues or externals.

Via the functions “changing accounts” and “log out” (on Windows systems accessible via the start button) more users are able to work at one working station. More information is granted by the O-IT.

In creating a password, the password instructions and rules from **Appendix 1** must be observed.

3.3 Clean Desk Policy

When leaving the workplace, the workstation computer must be protected by an entrance barrier (e.g. password, fingerprint) against access of third parties. Computers, which dispose a MED UNI image and are logged into their MUGAD domain, block themselves after 5 minutes of inactivity. At the end of each working day, all programs are to be orderly closed and the operating system is to be shut down.

All workplaces are to be secured by the employees so that unauthorized third parties cannot acquire any kind of insight or access to data. Monitor screens and printers are – if possible – to be positioned in a way that unauthorized third parties cannot acquire any kind of insight.

All printings and copies are after the making immediately to be removed from the respective device (printer, fax, etc.). Incorrect and/or incomplete printings and reproduction are to be destroyed.

Printings, copies or documents that are not required are to be disposed of correctly (data protection container, document shredder). In the reception area, it is to be ensured that no post or document, which contain personal data, is freely available.

3.4 Protection against Malware

All procured centrally computers are configured with an up-to-date virus scanner, which automatically reviews all incoming data and files. By the application of an anti-virus system, the penetration of harmfully program codes should be recognized and prevented. Automatic updates on the terminal device (e.g. workstation computer, laptop, smartphone, tablet) enable an automatic update of the virus definition on the computer. The automatic update cannot be interrupted as this may otherwise be a major security risk for the IT infrastructure.

On their own devices employees are to be ensured that the operating system is continuously updated and that appropriate virus protection is guaranteed.

The network is secured by a firewall, emails are reviewed by a central spam filter and anti-virus software. Information in info-mails regarding the handling of viruses and spams must be observed.

Medical technology laboratory devices or other devices with special requirements, on which virus protections cannot be installed, are not allowed to have access to the internet or respectively other measures to protect the network of the Med Uni Graz are to be set. For an exact clarification contact the O-IT (see point 2.1).

3.5 Use of local and mobile Devices of the Med Uni Graz

All in connection with the employment relationship handled data are saved on central (secured) servers (network drives etc.). The saving and handling of personal data as well as business and trade secrets on an unencrypted local or external data carrier, especially on local hard drives and USB-sticks, DVDs etc. is forbidden. The saving and handling on stationary workplace computers are acceptable, as long as the data is solely accessible to authorized employees of the Med Uni Graz and ensuring for an adequate data backup on a Med Uni Graz server.

A time-limited use of encrypted hard drives or USB-sticks for fulfilling business obligations (e.g. giving a lecture) is permitted. After being used the data is immediately to be deleted from the local data carrier.

The use of encrypted communication services is, as far as possible, to be preferred over the unencrypted services. The transmission of health data must be implemented by unencrypted communication services or saved by other suitable measures (e.g. isolated own network).

Mobile data carrier and terminal devices are constantly to be kept safe and can never be transmitted to third parties unlocked. Mobile phones are by means of an SMS-PIN and device code to be locked, not required functions should be deactivated (e.g. Bluetooth). Devices are not to be connected over the USB port to unknown sources. The application of a jailbreak or a rooting[1] is forbidden. The installation of certified apps (apps from the app store or Playstore) is permitted.

Med Uni-mails can be retrieved on mobile devices via Active Sync (exchange protocol). The used devices are thereby registered on the server.

3.6 Use of own (and private) Hard- and Software for Professional Purposes

The connection of hardware systems to a data network of the Med Uni Graz is solely implemented by the intended infrastructure. The unauthorized setup or use of additional connections (modems, router, switch, AccessPoints) without an agreement of the O-IT of the Med Uni Graz is inadmissible. The use of private hard- and software in connection with technical institutions of the Med Uni Graz and their wired network is not allowed. Temporary exceptions can be made by the O-IT but the private hardware must be registered in the network of the O-IT of the Med Uni Graz. The use of WLAN with private hardware is allowed.

General exceptions apply to the use of private computers for lectures and speeches in the WLAN as well as in specifically identified areas, such as libraries or student workplaces.

Data, which is in connection with an employment relationship, is not to be saved on private terminal devices or rather must be deleted after final use (consideration or completion of the

[1] Android and iOS are configured by the producer that not every data is visible or can be changed. This protects the operating system from harmful interventions but also limits the use. Those restrictions are removed by rooten or jailbreak.

process). The use of Webmail or applications over VPN access is allowed. The use of Owncloud or NextCloud clients on private devices is allowed as long as it is guaranteed that the for the synchronization of data used device is only accessible for authorized employees of the Med Uni Graz.

For the processing of personal data central applications, which are provided by the Med Uni Graz or the hospital, are to be used. Should this not be enough in a particular case, the preparation of own exports in data with the software applications provided by the Med Uni Graz is permitted. This data and the personal data processed therein are solely to be managed on the network drive of the Med Uni Graz or the hospital.

For the purpose of protection of hardware and the university network, it is only allowed to install software on computer systems of the Med Uni Graz, which are necessary for the fulfillment of business tasks. Therefore, it is preferred to use the software provided by the O-IT. Another software can only be used if it is necessary for area-specific business requirement. In case of uncertainty, the O-IT is there to help (see point 2.1).

The whole communication between the different sections of the Med Uni Graz or with external partners is solely implemented by controlled channels, which are carried by a specific protection system (Firewall). The installation or use of other communication connections (e.g. Modems), which are operated next to the network connections of the Med Uni Graz, are not permitted. If, in case of any specific circumstances, the installation of other communication channels is indispensable (e.g. operation of a Modem for remote maintenance purposes), the O-IT must approve of it. Every access of externals will be recorded.

3.7 Private Use of IKT

The Med Uni Graz allows all employees the private use of the “medunigraz.at” email address and Internet access. The private use is restricted by the Med Uni Graz in favor of the IKT application regulation of the federal government (Stammfassung: BGBl. II Nr. 281/2009 idgF), which is equal to be complied with by public employees and staff members.

Employees, however, have to consider company regulations (e.g. guidelines, transmissions, documentations) with regard to data and network security, which prevent the unlimited use of data (e.g. downloading from the internet, installing new software).

The dispatch of professional personal data from private email accounts or the dispatch of professional emails with a professional address of the Med Uni Graz to own private email addresses is not allowed. Automatic redirections of the professional email address to a private email address are not allowed.

3.8 Behavior in case of Loss or Virus Attack on Devices

In suspicion of virus attack, data espionage or other safety-endangering circumstances (lost USB stick or external hard drive, stolen contact info, lost laptop, violation against data protection regulations) it must be notified immediately to the data protection officer (email: datenschutz@medunigraz.at, tel.: 0664/88 96 17 48) as a possible data breach[2] must be registered within 72 hours by the person responsible in accordance with the rules of procedure of the rectorate to the supervisory authority.

If an email enabled terminal device (laptop, smartphone, tablet) gets lost or stolen, the employee has to deactivate the device immediately via Webmail. This also applies in case of loss of own terminal devices, if occupational data is processed on it.

3.9 Behavior in case of Withdrawal of Employees

In case of withdrawal of an employee, the correct transfer of professional data to the supervisor or respectively private data to the employee must be carried out in coordination with the employee and the supervisor. The O-It must be informed of the withdrawal.

4 Policies for Handling Personal Data3

4.1 Transmission of Patient and Subject Data

The use of professional email addresses within the secured KAGes or Med Uni network (or rather via Webmail application or Exchange server), “medunigraz.at”, “stud.medunigraz.at” and “klinikum-graz.at”, is allowed for the transmission of personal patient data in case of entitled purposes (e.g. cancer board, unusual fetal findings). The transmission between both mail servers is encrypted. A transmission of personal data to other places such as the state government or other universities is allowed in encrypted form but requires a still to be held examination by the O-IT to ensure that the mail servers communicate in an encrypted way. The transmission of personal and subject data to external receivers via email is only possible in exceptional cases and over secure and encrypted

[2] „**Data breach**“ is understood as an incident in which access to personal data becomes possible for unauthorized persons (e.g. loss or robbery of a data carrier, hacker attack, viruses or malware) but also an unintended data breach due to software errors in an Internet application or in an application program.

[3] **Personal data** is:

* direct personal data (names, local information, online identification etc.)

* indirect personal data, if data of a person can be allocated with the help of additional information or technical aids (pseudonymized data, IP address, genetic data etc.)

Pseudonymized data is personal data, that cannot be allocated to a specific person concerned without enlistment of additional information, as long as this additional information is kept separately and subjected to technical and organizational measures, which guarantee that the personal data is not assigned to an identified or identifiable natural person. Warning: Pseudonymized data is subjected to data protection.

Anonymized data is data that cannot be assigned to one person. Anonymous or anonymized data are excepted from data protection.

email connections, which must be set up by the O-IT. In this case the O-IT is to be contacted (see point 2.1).

4.2 Limitation of Processing

Personal data can only be processed so far as it is necessary for the fulfillment of business obligations. A transmission of personal data to third parties (those are natural or legal persons, who are not involved in the working process with which the particular employee deals with e.g. due to their job specification) has only to take place upon a specific order by a supervisor.

4.3 Ensuring Data Secrecy

Employees of the Med Uni Graz are bound to ensuring data secrecy in accordance with valid legal regulations (professional laws, hospital law, data protection law, criminal law) and obligated to the internal data secrecy formal obligation.

In case of a lawful and by the employer approved transmission of personal data to third parties (companies or natural persons) binding agreements (as an assignment processor or collectively responsible persons) are to be finalized.

If personal data independent from a contractual basis become accessible to natural persons (Med Uni externals) (e.g. as part of Boards etc.) those persons are obligated to ensuring data secrecy in accordance with the secret formal obligation for externals.

Appendix 1: Instructions and Policies for Passwords

If passwords are needed for an authentication in an IT system, the security of approach and access rights management of the system is conditional for the correct use of passwords. The users need to keep their password confidential. The password criteria can be found on the homepage (Intranet) or in MEDonline via password change.

Key rules around the creation of a password:

The choice of trivial passwords (e.g. “ABCABC”, “123456”) is to be avoided.

The password should contain at least one capital and lowercase letter and at least two figures and/or at least one special symbol.

Generally, no parts of words (more than 3 letters), which can be found in (German or English) dictionaries, should be used.

After the password change in MEDonline the saved password must be updated on all mobile devices, otherwise it leads to a blocking of the account.

Preset passwords (e.g. from the producer upon delivery of systems) must be replaced by individual passwords.

Key references on the use of passwords:

Passwords are not to be saved on programmable function keys or to be written down.

A password change is to be implemented, if the password becomes known by unauthorized persons.

Old passwords are not allowed to be continued to use after a password change.

The entry of a password must take place unobserve

Appendix 2: Measures of the O-IT for ensuring Data Protection

Access to and security of server infrastructure

All computer systems with a server function, including attached peripheral devices (consoles, external disks, drives) are to be set up in separate, secured rooms. The Med Uni Graz uses equipped server rooms for this. Access to these rooms by unauthorized persons is not possible. The rooms are secured by a key card or a key, only accessible by defined professionals and close automatically.

The central key management is made in coordination with the O-IT in the OE Med Campus: establishment and management. Therefore, it is regulated that a release to unauthorized persons is not possible and access is limited to those persons, whose work tasks require it.

Currently, all central servers are located in a server room of the Med Uni Graz on Med Campus.

On Med Campus, IT partners – as far as they have servers located in the server room – have access to the server room and the secured server racks. Only the area which the IT partners use can be locked.

Technical organizational measures guarantee an uninterruptible and safe operation.

Access control

In general, only those persons and members of the Med Uni Graz have access to the network and therefore to available resources of the Med Uni Graz, who previously obtained approval from the competent authorities. All use permission must be personal, this means anonymous user accounts are only allowed in justified exceptional cases (for example in laboratories, access to FTP or WWW servers, institutional or organizational demands, guest accounts).

The use of other person's usernames is not allowed. Normally access to the network is connected with access to data, application programs and additional resources. Therefore, the authentication of users of the network is of particular importance on all individual workstations at the university.

Redundancies in the administration of user names are to be avoided. The allocation of multiple usernames to one person within an IT system is only allowed in justified exceptional cases, for example for system administrators. The establishment and approval of a username takes place in a regulated procedure (process documentation in Aeneis-light).Which person in their functions will be authorized to use IT systems, IT applications or data is regulated by access rights. Users are only allowed to work with access rights, that are directly intended for the performance of their functions. The allocation or modification of all administrative and clinical applications, which must satisfy the legal requirements, is implemented by a written request.

The responsible staff must be informed in time of a necessary modification of entitlements of a user, e.g. as a result of modifications of their tasks, in order to illustrate the entitlement modifications in the system. OE managers or project managers are obligated to report access modifications on the file system or for applications of the O-IT.

System and network management

An appropriate recording, auditing and revision are essential factors of network security. An evaluation of such protocols with suitable aids allows an interference as to whether the range of the network satisfies the present requirements or systematical attacks on the network are recognized.

To secure the network adequate measures for recording are being taken.

The evaluation of protocol data takes place according to current legal regulations and regardless of individual persons (users). The Med Uni Graz reserves in case of an event (suspicion of committing a criminal act or grave misconduct) to evaluate the protocol data, as far as it is secured legally in the particular case.

Unsuccessful/incorrect attempts to access IT systems (server NW components) are automatically recorded. The modifying of important system parameters and also the shutdown or starting up of the system are likewise recorded.

Adequate measures are being taken in order to discover early on and localize overloads and disturbances in the network. It is regulated and ensured that only authorized persons can take hold of tools applied for this purpose. The group of authorized persons is restricted to the amount necessary.

Only known devices with the hardware address (MAC address) are operated in the Med Uni network. In order to ensure this and to regulate access to the network of the Med Uni a network management tool (ISE = Identity Services Engine) has been acquired. Hardware addresses of practiced devices in the network are deposited here. Web access enables administrators and IT partners an easy activation of devices.

The data network is structured in such a way that subnetworks are provided for different IT systems according to their particular protection needs. Systems with different protection needs are not operated in the same subnetwork. This will avoid that systems with high protection needs will be endangered at gateways by too little secured systems in the same subnetwork or by insufficient protection needs. Opposite it has also been achieved that access to systems with little protection needs will not be unnecessarily complicated, since other systems with little protection needs in the same subnetwork must be taken into consideration.

Data backup

Data backup is made with a documented data backup concept, which is appropriate for protection needs for the to be secured data and available in the O-IT. It provides information according to what criteria the data backup of data takes place and will be matched needs-based when setting up services between the O-IT and the IT partner or the responsible person. In case of personal data required minimum or maximum storage period will be considered.

The data backup concept includes all regulations for data backup (what, with whom, which method, when, how long and how secured). Storage of backup media is also regulated. All backups and storages of backup media are documented (date, implementation approach of backup/selected parameters, marking of data carrier, storage location).

Backup of data on servers takes place in an appropriate rhythm. It takes place in coordination with persons responsible for the server and applications for the particular server. When installing the server IT partners, persons responsible for the server and the application are determined. An own system is used for data backup that supports a backup for data, whose restoration takes more than a couple of days, by the generation principle.

Configurations of all active network components are saved in regular intervals.

Snapshots of virtual systems enable a fast restoration of systems after unsuccessful updates.

A backup server is specified in detail in the O-IT internal backup guideline.

The consistency of data backup runs is ensured, this means the readability of data backup is reviewed.

Documentation

The O-IT applies documented processes for tasks in their area of responsibility. Process descriptions are developed with help of the tool “Aeneis-Light”. A service catalog provides information on offered services. These include the following information:

- Process description
- System overview and network plan
- Interfaces to other processes
- Data description

Furthermore, the following areas have been documented internally:

- Representation regulations, in particular in the administration sector
- Access rights