Guideline for mobile Working and Home Office

Status: April 2019

Introduction

Modern end devices (smartphones, tablets, notebooks, etc.) make it possible to carry out business tasks not only in rooms and buildings of DESY, but also on the way (e.g. in the train or in the waiting area at the airport), on business trips (meetings, conferences, stay in other research institutions), or from home. Since a mobile working environment does not always provide the same basic conditions (confidentiality, working environment, etc.) as the DESY offices, some regulations have to be observed, for example to meet the requirements of data protection. This guideline informs about risks that arise from mobile working and gives recommendations for action to reduce these risks, but does not include aspects of workplace ergonomics and general safety.

Environment

Adequate working Environment

Choosing a suitable working environment is the first important step. It should be chosen in a manner appropriate to the scope of work and the security or confidentiality requirements. The mere processing of e-mails is to be evaluated differently than the creation of a certificate, for which additional sources of information (documents) may be required.

Especially when processing confidential information, it must be estimated whether third parties may become aware of it and what damage this may cause. This applies, for example, when telephoning in public, during conversations, for example in the train or when working on the computer in the train or in the plane.

The reading of confidential information on screens by third parties can be prevented, for example, by attaching privacy screens to the computer display.

Furthermore, a reasonable amount of space should be provided for the work, so that confidential information on printouts, for example, is not freely visible to third parties. If it is not possible to create a confidential work environment, confidential data should not be processed.

Working with mobile Devices

Another important step is to choose the right way of working. Here it has to be decided whether the data is processed and stored directly on devices within the DESY network

or whether the processing and storage of the data must be carried out locally on the mobile device, since a trouble-free network connection cannot be assumed or large amounts of data must be transferred.

In principle, a mode of operation is preferred in which the data remains on systems at DESY and the terminal devices only have access to them.

VPN vs. SSH

If connections to the DESY network are required, the choice of the appropriate access must be determined. This depends, among other things, on the type of terminal device with which the connection is established and which infrastructure is to be used within DESY.

VPN (Virtual Private Network) connections should basically only be established with end devices administered by DESY or comparable end devices. Otherwise connections tunneled via SSH (Secure Shell) are preferable. These can be used to use DESY internal working environments, e.g. those of a terminal server.

See also: http://rechnersicherheit.desy.de/regeln_und_empfehlungen/ssh_versus_vpn/

Local Storage vs. Data Storage at DESY

You can effectively counteract the potential loss of confidential information by processing this data only within the DESY network and not taking local copies with you. To do this, connect to the DESY network via a suitable path (VPN/SSH) and process and save the data directly on the systems in the DESY network.

Ensure an appropriate working environment (see above).

If local storage of confidential information cannot be avoided, suitable measures (e.g. encryption of folder contents under Windows using the extended attributes of the folder properties) must be taken to ensure that unauthorized persons cannot access the data, e.g. if the end device is lost.

End Device

Regular updates for operating system, applications and antivirus programs

Be sure to use only devices that have an **up-to-date operating system** that is still supported by the manufacturer and is **patched with the latest security updates**, i.e. all available security updates have been applied and the system has been restarted if necessary.

The same applies to the applications you use. **Make sure that the license conditions are observed.** Under certain circumstances, you may not use software that you have installed on your private end device for business purposes.

The use of an **up-to-date anti-virus program** is strongly recommended, and even required on devices running Microsoft Windows. Update your antivirus program signatures regularly, at least once a day.

Use of private End Devices

The use of centrally administered DESY systems is preferable to the use of private end devices. If private devices are used, they must meet the necessary security requirements (current operating system with all necessary security updates, current application software). The licence conditions of the installed software must be observed. If necessary, the manufacturer's license terms exclude the use of privately purchased software for business purposes.

When using private devices, it is advisable to separate business from private use, for example by creating a separate account/profile. This ensures a better separation of the data generated by business activities from the data from private use. If further business use of the device is no longer necessary, the profile should be deleted.

Use of third-party Systems

Occasionally, you may need to access third-party devices to perform business tasks. Please note the following points:

- It has to be assessed whether the security level of the end device is adequate for the planned task performance (How and by whom is it administered? Is it up-to-date?). If this is not the case, the device must not be used.
- After the work is done, close all used programs and log off. Existing connections to DESY services or systems must be terminated.
- Autocompletions should be disabled and passwords should not be saved.
- Temporary and cached data should be deleted. If you view files using a Web browser, for example, copies of the document are usually stored locally. These should be deleted. This can usually be done using the settings menu of the Web browser.
- If copies of data are stored in the temporary directory, these should also be deleted. The directory of temporary files can be reached under Windows by opening at the command prompt (Win key + R) and typing %TEMP%.

Data Carriers and Documents

Verschlüsselung von Datenträgern mit vertraulichen Inhalten

If confidential data or personal data are carried on data carriers, they must be adequately protected against possible access by unauthorised persons, e.g. after loss of the data carrier.

This can be achieved by encryption, the easiest way is to save them in a password-protected zip file or, under Windows, in a folder whose contents are automatically encrypted (setting via the Extended Attributes under General Properties).

For smartphones and tablets, encryption of the entire memory can often be easily enabled via the system settings.

Keeping Data Carriers and Documents

Documents and data carriers should always be kept in such a way that they are adequately protected against access by unauthorised persons and are not left lying around. This also means that rooms where these documents are kept must be adequately secured against unauthorised access in case of absence.

Leaving devices / documents

If, for example, you have to leave your equipment or other documents unattended for a short time during a conference, precautions must be taken to make unauthorized access to the equipment or documents reasonably difficult. These precautions include locking the screen and putting documents together. In the case of longer absences, additional mechanical security measures (Kensington lock) are to be provided to prevent the theft of the device, mobile data media or documents or make it sufficiently difficult.

Data Backup

Regular data backups are also required when working from home or on the way. This can be done either by storing data only on central DESY storages and thus automatically backing it up, or by creating independent backup copies. Here, the requirements for confidentiality and the regulations for disposal must also be taken into account (see Disposal). You must ensure that no working copies that are no longer required remain on storage media after the work is done.

Disposal of Documents and Data Carriers

If documents, printouts or data carriers are no longer required, they must be **disposed appropriately**. This can be done, for example, by mechanical destruction (shredding). Possible storage periods must be taken into account.

If appropriate disposal is not possible on the way, the documents or data carriers must be disposed at DESY via the usual ways.

More about the disposal of data carriers:
http://datenschutz.desy.de/regeln_fuer_desy/datentraegerentsorgung/index_ger.html

More about the disposal of documents:
http://datenschutz.desy.de/regeln_fuer_desy/dokumentenentsorgung/index_ger.html

Miscellaneous

Use for private purposes

The use of the resources provided by DESY is for business purposes. Any other use for private purposes is only permitted in accordance with the DESY User Regulations for IT Systems.

Timely reporting of losses

If hardware is lost, a corresponding message must be sent in real time. Details can be found here: http://rechnersicherheit.desy.de/themen/stolenhardware/index_ger.html

Encrypted protocols

When logging on to services, make sure that your logon data is only transferred via encrypted protocols. This also applies to the exchange of confidential information.

DESY Information on private Devices

DESY-internal information may in general not be stored on private end devices. Should this be necessary in exceptional cases, please make sure that possible working copies or temporary files are deleted, preferably overwritten.

Deleting Documents Downloaded for Viewing

Regularly delete files from your download folder, your web browser cache and the TEMP directory of your operating system that you no longer need. Under Windows, you can change the directory and manually delete temporary files by pressing "Win + R" and then typing %TEMP%in. Do not forget to empty the recycle bin as well.