“Emergency” Home-Office
Information and help for data protection

The corona pandemic is changing everyday life. For many UPB employees, the workplace has also at least partially shifted to the home, which enables us to maintain the University’s ability to function during this time.
A big thank you to everyone who has made this possible at short notice and often without much preparation.
Under these conditions, data protection presents us with particular challenges. In the following you will find information and assistance on how data protection and data security can also be considered in the “emergency” home office.

Physical transport of paper documents and mobile devices

Official paper documents and mobile devices that contain personal data and / or confidential information must be transported securely between the office and the home workplace and vice versa. Please find a way to transport these locked and choose the most direct route between the home and office and vice versa.

Entrance and access protection

Possible measures:

If possible, the home workplace should be used only by you. Please do not work in public spaces (e.g. in cafés).

Personal data and confidential information, which are or have been processed in the context of the performance of official duties, **may not be mixed with private data**. An official computer (notebook) should preferably be used. In the event that **private devices** are used, business content with personal data and confidential information must be protected against access by other people. In this case, please set up a separate account for business use and protect this account with a password. Please use the latest operating systems with security updates. Current virus scanners protect you against harmful software.

The data should be **stored encrypted if possible** and should be **securely deleted after transmission** to the official network. (Don't forget to empty the trash, too.) All data should be securely deleted after the end of the working at home phase. The **IT equipment** provided for business purposes **cannot be used for private purposes**.

The **connection** to the UPB must be made via secure connections. Most applications (email, PAUL, PANDA, ...) can only be used encrypted (HTTPS). A **VPN connection** additionally protects the data. Some services can only be used from outside the university with a VPN connection.

Please ensure that all business devices and storage media used for business purposes are **protected against unauthorized use and access** to the personal data and confidential information contained on them. In this context, it is also important to adjust the **screen** so

that household members and other third parties cannot see the data and information (e.g. through windows on the ground floor).

When you leave your workplace, please activate a **screen lock** that can only be unlocked with a password that is only known to you. It is also helpful to additionally set up an automatic screen lock, which activates the lock after at least 5 minutes.

The **installation of new software** on official devices may only be carried out in consultation with the organizational unit.

In order to ensure no data loss due to unauthorized access, external data carriers (external hard drives, USB sticks) with which data are transported should also be encrypted.

E-mails from central administration and from the IMT and vice versa, also between IMT and central administration, can be sent without any problems.

Other business e-mails that contain personal data and / or confidential information should be sent using **state-of-the-art encryption technology** if they leave the domain of the e-mail server.

Please never forward business e-mails to **private e-mail inboxes** (i.e. no use of gmail, gmx etc. for business e-mails).

An exchange of personal data and confidential information with official content may not take place via **messenger services** (e.g. WhatsApp) or other external services.

If possible, do not print documents that contain official content with personal data and confidential information at your **home workplace**. If this is absolutely necessary for the completion of official tasks, it must be ensured that the printouts are taken out immediately and stored or destroyed appropriately on site. In such cases, please disconnect the printer from the Internet.

Storage of paper documents and mobile devices

Business paper documents and mobile devices that contain personal data and confidential information **must be kept protected**. This means that other household members or third parties cannot have access.

Storage

The storage of personal data as well as other confidential information that is or has been processed in the course of fulfilling official duties must always take place in the **directories / folders of servers or in the central IT systems of the UPB** that are available for the specific user.

If an internet connection to the central IT systems and thus storage on the IT systems is temporarily not possible, an exception can be made: In these cases, **local storage** of the data and information on the devices used at home may take place if it is ensured that this data is

stored encrypted on the data carriers used. Please transfer the data to the central IT systems as soon as possible.

Destruction of paper documents

If you need to destroy paper documents that have official content, including personal data and confidential information, please **do not select your wastebasket**. Destruction in accordance with data protection must be based on the requirements of DIN 66399-2 (e.g. shredders with minimum security level 3). If such options are not available at home, please keep the documents locked and, if possible, dispose of them at the official workplace in accordance with data protection regulations.

Telephony
If you are dependent on a private telephone, set up a forwarding of the business number if possible.

If the phone numbers of the incoming calls are transmitted, please delete them regularly on your device.

If you are calling on your own private device, we advise you to **suppress (block) the number for outgoing calls**.

Notification in the event of a data protection incident

Possible data protection incidents are to be reported to the office and the data protection officer as soon as they become known. **Contact** should in particular already be made if there is an assumption that the confidentiality of data may be at risk and / or that a third party has or had unauthorized access or access to personal data and / or confidential information (e.g. lost or forgotten notebook on the train, a stolen / lost bag with data media and / or official paper documents, stolen / lost notebook etc.) The office must also be immediately informed of any security gaps that have been identified. An (information security) incident is reported via the **UPB ticket system** at: https://www.uni-paderborn.de/universitaet/informationssicherheit/informationssicherheitsvorfall/.

We hope to have given you valuable information. Take care of yourself and stay healthy.

The data protection officer Eva-Maria Wicker is available to you as the contact person.
Paderborn, 5.6.2020