UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Policy for the use of Sciebo

Area / Project:	Information Security
Author(s):	AG IT Security, Incident Team
File storage:	Sciebo
Version / Stand:	Version 1.0, 2.7.2020

1 Introduction

Sciebo is a cloud storage service in NRW, operated by universities for universities and financially supported by the state of NRW. The service allows all employees and students of the participating universities to process data in Sciebo (e.g. save, modify, share, upload and download). With the help of software on desktop and mobile devices, files stored on different devices can also be synchronized automatically. Furthermore, it is possible to access the data with all common web browsers. Moreover, Sciebo allows to share stored files with other users of Sciebo in Sciebo and with any other person via a link.

2 Scope

This policy regulates the official use of Sciebo and the associated processing of data of the university. It is binding for all employees of UPB.

3 Objective

The aim of this document is to define binding rules for the use of Sciebo at UPB. These rules ensure that the UPB and the persons concerned are not exposed to any unnecessary risks when using Sciebo. More specifically, the circumstances under which a file may be stored in Sciebo shall be regulated. In addition, general behavior in dealing with Sciebo is defined in the following section.

4 General behavior in dealing with Sciebo

In addition to the selection of data that may be processed in Sciebo, there are other behavioral principles that must be considered, which are defined in the following two subsections.

4.1 Permitted use

According to the terms of use of the service, the use of Sciebo is only permitted for the purposes of study, teaching, research and administration.

Personal data may only be processed in Sciebo in accordance with the GDPR if there is a viable legal basis for the processing (lawfulness of the processing) and the security of the data processing is guaranteed. The processing principles pursuant to Art. 5 of the GDPR and the conditions for the lawfulness of processing pursuant to Art. 6 of the GDPR apply. In order to mitigate risks to the rights and freedoms of data subjects affected by a processing operation, appropriate technical and organizational measures shall be implemented with regard to the processing (Art. 25(1) and 32(1) of the GDPR). The selection of appropriate measures depends on the risks present in the individual case. Personal data with a very high protection requirement (e.g. health data) may not be processed in Sciebo pursuant to Art. 9(1) of the GDPR.

4.2 Check the consequences before processing

It is easy to share data stored in Sciebo with other persons and to automatically transfer files to other devices if necessary. Therefore, before storing data in Sciebo, always consider the consequences of the processing first, especially to which persons and to which devices the data will be automatically transferred.

5 Suitable files for Sciebo

In order to decide whether a file may be processed in Sciebo and which additional protective measures may have to be taken, information in the files is classified into the categories "Normal

protection requirement", "High protection requirement" and "Very high protection requirement" according to its protection requirement with regard to the protection goals confidentiality and integrity.

The requirement to protect availability is not considered because storing a file in Sciebo does not have a decisive positive or negative effect on the availability of the file, as described in 6.2.

To perform this classification, please refer to the "Guideline for classifying the protection requirement for information". Often, you can also determine the protection requirement in a simplified manner using the list "Classes of information and their usual protection requirement".

Processing of data in Sciebo is allowed without restriction if its protection requirement is normal. It is not allowed if the protection requirement is to be classified as very high. If the protection requirement is high, the additional protection measures described in 6 must be implemented during processing.

	Normal protection requirement	High protection requirement	Very high protection requirement
Confidentiality	Allowed	Only allowed with the protective measures described in 6	Not allowed
Integrity	Allowed	Only allowed with the protective measures described in 6	Not allowed

6 Technical limits of Sciebo

The operators of Sciebo make every effort to ensure the protection goals described above for the files of users. Nevertheless, adherence to the protection goals cannot be guaranteed in the case of a high or very high protection requirement. Such files may therefore not be processed at all, or only in accordance with the additional requirements described in the following sections and with the following measures.

6.1 Ensure confidentiality and integrity

Since Sciebo does not ensure confidentiality or integrity of stored files, you need to take measures yourself before storing files with high protection requirements.

To ensure the confidentiality of files, you must encrypt them with suitable software before storing them in Sciebo. For help in selecting suitable software for encrypting files, please refer to the IMT help pages on "Using data encryption".

File integrity can also be ensured by using appropriate file encryption software. To ensure integrity, you can therefore also follow the steps on the IMT's help pages on "Using data encryption".

6.2 Ensure availability

There is no guarantee for the permanent availability of files in Sciebo, also protection against accidental deletion is not available. As a UPB employee, this means that you must ensure the availability of files yourself. You can find help on the IMT help pages on the topic "Keeping your data secure”.

6.3 Ensure data minimization, non-concatenation, transparency and intervenability

If personal data is the subject of information, the other demands of data protection law must also be observed, namely data minimization (data is processed only to the extent necessary), non-concatenation (data processed for different purposes may not be combined), transparency (recognizability of who processes data from whom for what purpose, through which systems and in what way) and intervenability (ensuring the rights of data subjects (e.g., information pursuant to Art. 15 of the GDPR and, if necessary, implementation of required measures)). Users must meet these demands themselves. All users can obtain advice on determining individual data protection risks from the UPB data protection officer.

7 More information

You can find more information at

- hochschulcloud.nrw/en/ about Sciebo
- hilfe.upb.de about Sciebo, data encryption, data backup and much more
- www.uni-paderborn.de/en/university/data-protection on dealing with data protection risks
- www.uni-paderborn.de/en/university/information-security on protection requirements of information and data