UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Supplementary questions for reporting a loss of data media

(dated: 19.08.2021)

Information and data

The data carrier contained information with the following protection requirements:

- ☐ Normal (e.g., official contact data, time sheets, students' homework)
- ☐ High (e.g. billing documents, corrections, grades, private contact data, confidential content from e-mail inboxes with external communication partners),
  For example:

- ☐ Very high (e.g., medical / health data),
  For example:

See classifications of information and their common protection requirements
https://www.uni-paderborn.de/fileadmin/informationssicherheit/20200702_Schutzbedarf_Informationsklassen_v1.pdf

Encryption

- ☐ The data was stored in encrypted form.

  The following technology was used for encryption
  - ☐ Encryption with an encryption module integrated in the data carrier.
  - ☐ Device or data carrier encryption by operating system, e.g., Bitlocker (Windows), FileVault (macOS), dm-crypt / LUKS (Linux)
  - ☐ File encryption using third-party tools (e.g.: Cryptomator, Veracrypt, Boxcryptor, AxCrypt, or similar).
  - ☐ Document encryption using password protection (e.g. Word, Excel, PDF reader, or similar).
  - ☐ Other:

Authentication / password security

The weakest password or the weakest authentication method used to decrypt the data is relevant here.

- ☐ The password is only used for this specific application.
- ☐ The length of the password is shorter than 8 characters.
- ☐ The length of the password is equal to or longer than 12 characters.
- ☐ The password contains expressions found in a dictionary (including proper names).
- ☐ The password contains upper and lower case letters.
- ☐ The password contains digits.
- ☐ The password contains special characters.
- ☐ A second factor (e.g. smartcard) is required and it was not lost (still in possession)
- ☐ The device was switched on or in standby.

Further information

BSI fact sheet Secure Passwords
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf