Richtlinie für Passwörter / Guideline for passwords [EN]

The Gauß-IT-Zentrum as the central institution of the Technische Universität Braunschweig provides a variety of IT services for authorised members and affiliates of the university.

To ensure authentication, authorisation and security, it is usually necessary to log in to the systems using a combination of a central TUBS-ID and password.

Security

Extensive authorisations are linked to the central TUBS-ID. In order to maintain security in the IT systems of TU Braunschweig, it is therefore essential that users also use appropriately secure passwords and keep them secret. This password policy has therefore been created to ensure an appropriate level of security. Users of the central TUBS-ID must comply with this policy.

Appropriate handling is recommended for the decentrally managed systems.

Password rules

Passwords must have a certain level of complexity so that they cannot be determined quickly.

The passwords for the central TUBS-ID must therefore be composed as follows:

The password must contain characters from at least 3 of the following 4 groups:

1. Capital letters: **A - Z**
2. Lower case letters: **a - z**
3. Digits: **0 - 9**
4. Special characters, only the following: **+ _ . , : -**

The following also applies to the password:

- It must be 12 to 30 characters long
- It must not begin with a minus sign (-)
- It must not be the same as the last 10 passwords
- It must contain each selected group at least twice (e.g. 2 digits, 2 special characters, etc.)
- It must not contain parts of the name or TUBS-ID that are longer than 2 characters

These parameters are technically checked as far as possible when the password is changed via the website. This also applies analogously to changing the password in the administration domain for the accounts in the administration domain.

As a further addition to ensure the required security, the password should be changed regularly.

Safe handling

The following rules must always be observed when dealing with TUBS-IDs and passwords:

- The personal TUBS-ID must not be shared with others
- A password must never be communicated openly (telephone, e-mail, etc.)
- The password must not be communicated to third parties (not even to service staff and administrators of the Gauß-IT-Zentrum)
- The same password should never be used for several TUBS-IDs
- The TUBS-ID with the password must not be stored on external systems
- A workstation computer must be locked with a password when leaving it

Behaviour in the event of a suspected attack

If there is any suspicion that the password has been compromised, i.e. attacked in any way, the password must be changed immediately using the usual channels. In addition, the IT Service Desk must be contacted immediately.

Created 2025-08-19 16:47:52 UTC by NTS
Updated 2025-08-19 16:55:07 UTC by NTS