**Instruction for external users with a "central login" at the
URZ (computing centre) of the TU Bergakademie Freiberg
(right of use according to § 6 (2) (3) (4) of the
Administration and Use Regulations of the TU Bergakademie Freiberg Computing Centre**

1. The user has taken note of the above mentioned administration and usage regulations of the university computer centre
   (https://tu-freiberg.de/sites/default/files/media/universitaetsrechenzentrum-149/dokumente/benutzungsordnung.pdf)
   as well as the operating regulations for the data communication network of the TU Bergakademie Freiberg (network regulations,
   https://tu-freiberg.de/sites/default/files/media/universitaetsrechenzentrum-149/dokumente/netzordnung.pdf) and commits himself to comply with these regulations.

2. The allocation of access to external parties (non-members and non-affiliates of the TU Bergakademie Freiberg) is based on a purpose of use that is in the interest of the TU Berg-akademie Freiberg. If this purpose of use ceases to exist, the access may no longer be used.

3. When applying, the desired time limit and the purpose of use must always be stated in accordance with the purpose of use. Should the purpose of use last longer than the time limit, the time limit can be extended by an authorized employee before the account expires at the service desk by mail (servicedesk@tu-freiberg.de). A written confirmation by an authorized employee of TU Bergakademie Freiberg can be requested by the URZ.

4. The use may only take place within the scope of the purpose of use. The use of network resources (e.g. applications, database accesses etc.) which are intended for internal use only or, due to special licence conditions, only for members or affiliates of the TU Bergakademie Freiberg is prohibited.

5. The password for initial access provided with the confirmed user registration must be changed immediately (within one week at the latest) in accordance with the applicable rules using the IDM portal at https://idmweb.ad.tu-freiberg.de. This personal password must be kept secret and must not be disclosed to anybody, not even the system administrators or employees of the URZ.

6. The disclosure of the personal user access (login and password) to others is prohibited. Violation can be punished by immediate withdrawal of the user authorization. The owner may be held liable under criminal or civil law for any damage caused by the disclosure of the credentials.

7. If confidential information becomes accessible to external users due to special circumstances, it must be kept secret and neither be disclosed nor made available to third parties. The concluded confidentiality agreement is expressly referred to.

8. Upon termination of the user relationship, all user data will be deleted. For the backup of this data before the account expiration, the user himself is responsible.

I took note of the regulations:

_____

Date   Given Name / Surname   Signature

(The registered user gets the original document, a copy of this will be kept with the registration form at the URZ.)