Terms of use for the “LSDF Online Storage” service

As of October 11, 2017

1. Services and user group

The “LSDF Online Storage” (LSDFOS) service offers users of the Karlsruhe Institute of Technology (KIT) access to a data storage that is intended in particular for the storage of scientific measurement data and simulation results from data-intensive scientific disciplines. The LSDF OS is operated by the Scientific Computing Center (SCC). Access is guaranteed via standard protocols. The data is secured and protected according to the current state of the art. The service is not suitable for storing personal data.

2. Storage space and intended use

Each user receives a directory for personal use only. In addition, project directories intended for shared use by groups of users will be set up upon request.

The setup and size of the available storage space is determined by agreements between the users and the service operator and is technically implemented through quotas. As a rule, a “data management plan” (DMP) is developed and filed in coordination with the user institute and representatives of the service operator. The DMP includes at least

- the name of the institute or facility,
- the name of the project,
- a short description of the project for which the storage is to be used,
- one or more contact persons with contact details of the contact persons,
- the amount of data expected in the next 3 years and
- the expected storage period.

The DMPs are used for reporting and when applying for funds for the operation, maintenance and expansion of the LSDF.

The LSDF OS storage space is currently generally available free of charge. Terms of use for the “LSDF Online Storage” service It is expected, however, that LSDF OS services will be rewarded accordingly by including a passage in scientific publications. A current formulation of the passage can be found on the LSDF OS website.

The operator retains the option of charging market-conform costs for the use of the LSDF OS service in the future. Possible changes to the Terms of Use in this regard will be announced as described under point 8 (Changes to the Terms of Use).

3. Data protection

When registering to use the LSDFOS, the following information about the user is transmitted in encrypted form to the service operator at KIT and stored there:

- First and Last Name
- e-mail address
- Name of the organization
- Unique user ID (EPPN & persistent ID)
- Status of the users (students, employees or guests)

The regulations of the State Data Protection Act (LDSG) and area-specific data protection regulations (in particular TKG, TMG) as well as European data protection guidelines in the currently applicable versions are observed. Furthermore, the current rules of the “Regulations for Digital Information Processing and Communication” (IuK) at the Karlsruhe Institute of Technology apply (available at http://www.scc.kit.edu/sl/iuk-regulation).

4. Data security

Access to the LSDF OS is guaranteed via the standard protocols SSH, SCP, SFTP, NFS, HTTPS (or WebDAV) and CIFS (Samba). The communication between the user's end devices and the LSDF OS is usually encrypted. When using the NFS protocol, communication is not encrypted.

Access is protected by username and password. When using the NFSv3 protocol, access is protected exclusively by releasing directories for individual IPs/end devices. The responsibility for implementing and enforcing effective access control on the end device that imports directories using the NFSv3 protocol lies with the end device administrator.

The saved data is stored unencrypted on LSDF OS storage systems. Data access is initially limited:

- In the personal user directory to the owner of the user directory.
- In project directories to all users who belong to the assigned user groups. The group memberships are managed by the group representatives of the institutes.

It is the user's responsibility to check the access rights to their data.

All data is regularly backed up to tape to enable disaster recovery in an emergency. Users do not have direct access to this backup.

In order to enable LSDF OS users to restore older versions of files, the service operator regularly backs up versions of the file systems as so-called snapshots. The storage space required for this is at the expense of the agreed quotas of the user or user group.

5. User and group identifiers

All stored data must be able to be clearly assigned to a user or a user group using the user identifiers (UID) and group identifiers (GID) assigned by the KIT-IDM or bwIDM system. The use of other IDM

systems is not supported. It is the responsibility of each user to ensure that data is only stored with their personal UID and a valid GID.

Data that was stored with an incorrect or incorrect UID or GID will be handed over to a person responsible for the project in consultation with the project manager or the OE management in collaboration with the responsible ITB.

6. Deprovisioning

Personal user directories will be deleted within 3 months of deactivating the user account.

User data that is located in project directories is treated as follows: Users who leave their institution or the project must determine what will happen to their data before leaving. If data is handed over to a person responsible for the project or institute, the SCC offers assistance with the change of ownership. If no determination is made, the data will be handed over to a person responsible for the project in consultation with the project manager or the OE management in collaboration with the responsible ITB. This person receives full access to the data.

7. Availability

The service infrastructure systems run permanently in 24/7 mode. On weekdays from 9 a.m. to 5 p.m., the service operator aims for a maximum response time of four hours to user inquiries.

KIT generally strives for the highest possible service availability. Planned service interruptions, e.g. for maintenance work, will be announced in advance with five working days' notice. The service operator reserves the right to interrupt service without notice for important reasons (e.g. security updates).

8. Changes to Terms of Use

The service operator is entitled to change the terms of use for valid reasons. Users will be informed of the changed conditions and must agree to them within 3 months in order to continue using the service. If the user does not agree to the changed terms of use in a timely manner, his user account will be deactivated.