DKRZ[1] Long Term Archive[2]: Risk Assessment

Revision History

Revision	Author	Scope
2018-10-22	DKRZ Datamanagement	public release

Policy Statement

Data Savety and Security is part of the operations and planning of DKRZ-LTA to support climate research.

Intended Audience

DKRZ LTA Managing Director, DKRZ Data Manager, DKRZ-LTA Users.

Motivation for This Document

An important part of the DKRZ Long Term Archive's (DKRZ-LTA) tasks is data security, data safety, and the assessment of possible data risks.

This document aims to describe data security and safety measures and to review the remaining risks for the data (risk assessment).

Security

Regarding unlawful physical or logical access to the data, WDCC is under the auspices of DKRZ and uses the DKRZ storage infrastructure for its data holdings. In collaboration with DKRZ all necessary precautions are taken to ensure safety and security of DKRZ-LTA data holdings. This equally refers to integrity, confidentiality, and availability of the data.

General Security

The status of data availability is displayed to the user on the WDCC web page with green/yellow/red marks in case of possible unavailability of the tape system. In case of longer lasting problems a warning and information page can be displayed. DKRZ takes all the usual technical measures to protect its long-term archived data against hacker attacks.

All data is backed up to the Max Planck central computing facility (RZG) at Garching near Munich, 800km away from WDCC. This backup can serve for business recovery and continuity in cases of logical data corruption and physical fails of integrity or other disasters. The copy at RZG is not accessible even for most of the staff members.

Physical Security

Only trained DKRZ (and RZG Garching) staff has access to the storage infrastructure which is in an especially secured environment. Here, all accesses to the machine hall are controlled, logged, and monitored. State of the art fire prevention and protection systems (like an oxygen reduction system) are in place.

For the case of a power outage, an Uninterruptable Power Supply (UPS) is installed.

Logical Security

The access to the WDCC data is audited. So depending on the nature of the problem, the according log files can be used to find out staff, users, or third parties who might be involved in any critical incident.

In addition, password and firewall protections are in place.

After every write process to tape, the data is re-read to be checked for bitwise identity. On a regular basis the data objects are copied onto new tape media to overcome media deterioration. In addition most frequently accessed data is cached on disk devices.

Risk assessment

A self-assessment of the different risks for data at WDCC yields the following assembly:

- Unlawful physical third party access: low risk, as access to the building as well as to the machine halls is controlled by access chips.
- Unlawful logical access by third parties: some risk. An LDAP access control system is installed at DKRZ. WDCC is integrated into this system. However, any password depending system depends on the reliability of the clients. Write access, i.e., filling and changes of data and metadata can be undertaken by trained DKRZ staff only.
- Violation of confidentiality: very low risk as a) the bulk of the data is completely open and distributed by free download and b) there are virtually no personal data kept at WDCC, except citation data. DKRZ restricts data access for data users and providers to read-only permissions.
- Power outage: low risk, there have been few incidents during the last decades but they mostly were easily buffered by the Uninterruptable Power Supply (UPS).
- Technical and staff faults: low risk. However, they never can be excluded completely. Therefore access to the metadata base and data storage is possible for well trained staff only.
- Especially smoke and fire risk: At WDCC the local storage of the data is under a reduced oxygen atmosphere. This lowers the above risk substantially and requires a denial of access for everybody except very few staff members.

All in all, the openness of most of the data lowers any risks of confidentiality violations substantially, the external backup allows for complete recovery of WDCC data in case of corruptness.

Further policies

For all issues concerning WDCC's general data policies see the document *DKRZ-LTA Preservation and Storage Policy* which can be found, e.g., on docs.wdc-climate.de .

For all matters concerning general protection of personal data see the DKRZ website at https://www.dkrz.de/about-en/contact/en-datenschutzhinweise . This not only refers to data access by web browser but also by any API and by the jblob download tool.

Contacts

In case any questions regarding this preservation and storage policy arise please contact DKRZ-LTA user support at data@dkrz.de.