Computerome
Security Overview 2020

Security Based on Risk Assessment

As research projects using Computerome may have valuable scientific information or sensitive personal data, the security level of the system is set to accommodate the requirements for protecting these types of data, based on a risk-based approach.

The general physical and technical risks, as well as risk associated with people are therefore assessed on a frequent basis and appropriate measures are taken to uphold the security of the system, including the **confidentiality, integrity** and **availability** of data. This pamphlet describes the technical and organisational measures taken to maintain the general security of Computerome at a high level, and can be used as an input to the customers' risk analyses, or Data Protection Impact Analysis which some customers shall perform based on GDPR requirements.

Physical Risks

Physical risks comprise risks of natural disasters (flood, lightning and earthquake) machine failure (cooling failure, fire, hardware failure and power outage) as well as risk of unauthorised access to Computerome facilities, which are mitigated by the following measures:

- Computerome facilities are placed several meters higher than the critical threshold above the sea level, and are elevated above the ground level.
- Several lightning rods are installed around Computerome facilities.
- Fire and heat detectors, as well as automatic fire extinguishers are installed in server rooms and are serviced frequently.
- HVAC system is used to monitor the facilities by the central security office.
- Redundancy is built in computation, storage and network components to mitigate the risk of single node failure.
- Uninterruptible Power Supplies (UPS) are installed and serviced frequently, which in case of major power outage allow the system to shut down gracefully and avoid loss of data.
- Access to the facilities are controlled by 24/7 security service, and the facilities are double-fenced and monitored by surveillance cameras and infrared sensors.

DTU

Version 1, November 2020

Technical Risks

Technical risks are risks related to software and cyber attacks, which are mitigated by the following measures:

- Network and user group segmentations ensure that research groups are not able to access, or compromise other research groups or their data.
- Procedures for user management ensure users get access to the authorised research group(s) only.
- Two-factor authentication is a requirement for all users, including users with administrative rights.
- All successful/unsuccessful log-ins as well as access to data are logged and monitored for suspicious behaviour.
- Security Information and Event Management (SIEM) logs and monitors real-time data in several layers of the system such as CPU usage, disk I/O and user behaviour, in order to detect suspicious behaviour conducted by users or malicious software.
- In order to mitigate loss of data in case of software incidents or accidental deletion of data, the storage system uses an integrated snapshot solution to take hourly snapshots up to 26 hours back in time, daily snapshot up to one week back, and weekly snapshot up to four weeks back in time.
- Redundant firewall setup with sufficient bandwidth and dynamic IP black list ensures that known, suspicious IP addresses are blocked, in order to avoid a DDOS or similar attacks.
- Penetration tests are performed frequently to ensure the robustness of network and the IT system in general.
- For Cloud users, extra features are available upon request, including:
    - restriction on import and export of data
    - restriction of copy-paste function (of texts or files)
    - disabling internet access
    - direct access to user management, without Involvement of the Computerome staff

People

Risks related to human error, behaviour of staff, vendors or end users are mitigated by the following actions:

- All staff are required to document educational background and work experience prior to employment.
- To ensure compliance to laws and legal contracts, the staff are frequently trained in standard operating procedures, which regulate management of users, contracts, and the IT-system in general.
- Non-disclosure agreements or data processing agreements are signed with internal or external staff to ensure confidentiality of information.
- Logs from the entire IT-system is collected and stored centrally with read-only access to HPC staff.