

LUMI Technical and Organisational Measures (TOMS)

Title of document	LUMI Technical and Organisational Measures (TOMS)
Date of last change	24.06.2026
Version	1.0
Document owner	LUMI Operations Manager
Related documents	LUMI Terms of Use LUMI Personal Data Protection Agreement

General Principles

- **Segregation of Duties:**
Administrative responsibilities are divided among network, data center, and system administrators to minimize risk.
- **User Terms of Use:**
Users must agree to LUMI Terms of Use before accessing the service environment.
- **Shared Secret Management:**
Administration-level credentials are stored securely and managed through dedicated system management servers.
- **Layered Security Architecture:**
User access and system administration interfaces are segregated within secure network zones and protected by firewalls.
- **Contractual Basis:**
All data processing operations are based on written agreements with the data controller.
- **Role-based Access Control:**
Access rights are allocated according to roles and follow the principle of least privilege. CSC maintains its staff's access rights, ensuring they are limited to tasks that require access.
- **Access Management:**
Data controller retains control over its own staff's access rights.
- **Training and Awareness:**
CSC personnel receive continuous data protection and security training. Training records are maintained internally.
- **Confidentiality Obligations:**
All personnel handling personal data are bound by confidentiality agreements and comply with applicable data protection laws (such as the Finnish Act 1050/2018).



EuroHPC
Joint Undertaking



The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the Participating States FI, BE, CH, CZ, DK, EE, IS, NL, NO, PL, SE.

Leverage from
the EU
2014–2020



European Union
European Regional
Development Fund



- **Data Protection Officer:**
CSC has appointed a dedicated Data Protection Officer (DPO) to oversee data protection compliance.
- **Data Storage Location:**
All data is stored within the EU (Finland).

Measures to Ensure Confidentiality

- **Network Protection:**
Firewalling blocks access from the public Internet to login nodes and web user interface by default, allowing access with only specific secure protocols (SSH and HTTPS). For web user interface servers the default deny policy applies also to connections from the servers towards the public Internet.
- **Data Encryption:**
All data transfers between users and systems (including web interfaces and terminal access) are encrypted. The password hashes for user authentication to LUMI web user interface are stored encrypted in an external identity provider system outside of LUMI.
- **Filesystem Access Control & Data Ownership:**
Standard UNIX-based access management (user-group-other) is applied to all data stored in the LUMI filesystem. Data stored in project-specific scratch and projappl areas is accessible to all members of the respective computing project. Home folders are always restricted to be only accessible by the user. Users can further restrict access to their files within project areas, but cannot grant permissions beyond the default project-level access constraints.
- **SSH Key Management:**
SSH connections to LUMI are authenticated exclusively via SSH keys, which are centrally managed through the MyCSC portal (Finnish users) and on MyAccessID portal (other users). Users are required to register and manage their public SSH keys via these portals, ensuring controlled and auditable access.

Measures to Ensure Integrity

- **Vulnerability Management:**
The Services are being regularly scanned for vulnerabilities and other weaknesses. This means that CSC internal security team will scan the Services regularly in order to verify no unspecified network services or ports are available, and that no known vulnerabilities exist on the Services.
Security patches are being applied regularly. This means that the software is kept up to date with regular updates on all systems needed for the Services. Critical security patches are applied as soon as possible.



EuroHPC
Joint Undertaking



The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the Participating States FI, BE, CH, CZ, DK, EE, IS, NL, NO, PL, SE.

Leverage from
the EU
2014–2020



European Union
European Regional
Development Fund



- **Change Management:**
A formal change management process ensures all updates and changes are reviewed and implemented securely.

Measures to Ensure Availability and Resilience

- **Automatic Monitoring:**
CSC uses automated monitoring systems to detect and report service disruptions or anomalies to administrators.
- **Disaster Recovery & Backup:**
System configurations and data are version-controlled and replicated to ensure quick recovery in case of failure.
- **User Data Backup Policy:**
No backups are taken of user data stored in the home, projappl, and scratch areas of the LUMI supercomputer. Users are responsible for maintaining their own backups of critical data stored in these locations. Data in these areas is not covered by CSC's backup or disaster recovery processes.
- **Software Package Management:**
Operating system software repositories are locally mirrored to ensure the availability of necessary updates even if external sources are unavailable.
- **User Account Synchronization:**
User accounts are automatically synchronized with CSC's central user management system to maintain operational resilience.

Measures for Testing, Evaluation, and Assessment

- **Audits & Compliance:**
CSC conducts regular internal and external audits, including ISO 27001 audits, to evaluate the effectiveness of security measures.
- **Incident Management:**
Security incidents are managed according to defined operational processes, including analysis, response, and post-incident reviews.



EuroHPC
Joint Undertaking



The acquisition and operation of the EuroHPC supercomputer is funded jointly by the EuroHPC Joint Undertaking, through the European Union's Connecting Europe Facility and the Horizon 2020 research and innovation programme, as well as the Participating States FI, BE, CH, CZ, DK, EE, IS, NL, NO, PL, SE.

Leverage from
the EU
2014–2020



European Union
European Regional
Development Fund

