PUHURI

UNIVERSITY OF TARTU
High Performance
Computing Centre

# Technical and Organizational Measures of Puhuri Core and Puhuri Portal

## 1. Overview

The University of Tartu is hosting the Puhuri Core and Puhuri Portal instances, the functions of which are described in the Service Description.

This document describes technical and organisational measures to ensure information security and protect Personal Data in the High-Performance Computing Center (hereinafter: UTHPC) of the University of Tartu (hereinafter: University).

### Security standards

In providing the service, the UTHPC will comply with the requirements of the E-ITS[1].

## 2. Introduction and scope

2.1. UTHPC technical and organisational measures are based on the requirements and rules established by the University and the obligations arising from the Contract.

2.2. The basis for ensuring information security at UTHPC is the continuous assessment and implementation of information security measures and the training of UTHPC employees.

2.3. All UTHPC employees must familiarise themselves and follow UTHPC technical and organisational measures.

2.4. Technical and organisational measures apply to all data and information assets belonging to UTHPC that UTHPC uses to achieve its objectives or that are connected to networks managed by UTHPC.

## 3. Principles

3.1. UTHPC, as the owner of the information assets, selects adequate and appropriate measures to protect them.

3.2. Data and information assets shall be protected following the policies and laws of the UTHPC and the University, particularly those relating to data protection, human rights and freedom of information.

3.3. Each information asset must have a designated lead user responsible for implementing appropriate security measures to protect the information asset.

3.4. Non-public information shall be made available only to those with a legitimate right to access that information.

[1] https://eits.ria.ee/

3.5. Everyone granted access to information assets and data shall be responsible for their proper handling following confidentiality.

3.6. Data and information assets must be protected from unauthorised access.

3.7. Information assets are only available to those with the right to use them.

3.8. UTHPC will provide necessary security training for its employees.

## 4. Obligation of confidentiality

4.1. The confidentiality requirement applies to confidential information and UTHPC employees due to legislation and agreements.

4.2. Information that is accessed by contract or law or that has been declared non-public on any other basis is considered confidential.

4.3. All UTHPC employees who come into contact with confidential data shall, as a minimum:

4.3.1. not disclose confidential information which has become known to him or her unless it is required by law or necessary for the performance of his or her duties;

4.3.2. comply with applicable data protection legislation and procedures;

4.3.3. comply with the requirements of the obligation of confidentiality both during and after the employment relationship.

4.4. If a third party performs the contractual obligation:

4.4.1. there must be a contract between the University and a third party, which parties sign before the contractor is granted access to the information assets;

4.4.2. The contract must contain provisions on confidentiality requirements.

4.5. Confidential data is processed on the UTHPC servers, and data transportation on data carriers is prohibited.

## 5. Access Control

5.1. Access rights are determined based on the minimum principle, which means that access is granted only to information assets to which access is necessary for the performance of work or use of the Services.

5.2. Granting, modifying and removing UTHPC employees' access rights is governed by the UTHPC Access Rights Rules.

5.3. The access rights of UTHPC employees shall be audited regularly, at least once a year, and the audit result shall be recorded.

5.4. When UTHPC employees' work responsibilities change, the access rights of the respective employees are reviewed, and the rights that are not necessary for the performance of the new job responsibilities are removed.

5.5. Upon termination of employment of a UTHPC employee, all rights of the respective employee will be removed, and the account will be closed immediately.

5.6. Administrative access to UTHPC resources is restricted to UTHPC employees.

5.7. Separated network and firewall rules and strong access credentials protect unauthorised access.

5.8. All UTHPC resource users have user roles that restrict their access to data related to their projects.

5.9. UTHPC resource user representatives have access, read and necessary modification permissions to their resources to make necessary changes to resources.

5.10. UTHPC resource user representative's access is limited via the firewall.

5.11. UTHPC internal and external support teams have read access to the resources they provide support.

## 6. System operations

6.1. UTHPC shall ensure that the service platform and components are updated.

6.2. Operating systems and applications are actively maintained. Unnecessary services are disabled or put behind the firewall.

6.3. UTHPC uses audit software to electronically monitor its networks, servers, routers, firewalls, and/or other UTHPC systems.

6.4. When making changes to hardware or software, the requirements established by the University and the rules established by UTHPC are followed.

## 7. Physical security

7.1. The University hosts all UTHPC network devices and servers in a closed Data centre.

7.2. Only authorised necessary UTHPC personnel with a special permit have physical access to the data centre.

7.3. The data centre is behind two locked fireproof doors that can only be opened with a personal smart card.

7.4. The data centre is under electronic surveillance, and when entering the Data centre, the security must be deactivated using a personal code.

7.5. Data centre electronic surveillance can only be deactivated if someone is physically in the server room.

7.6. All Data centre entries and electronic security deactivations/activations are logged.

7.7. To ensure fire safety, the university must follow the fire safety rules.

## 8. Availability and integrity

8.1. Maintenance of security measures, periodic reviews of regulations, daily monitoring of the working environment, periodic compliance checks of information security, response to changes and handling of information security incidents are necessary to ensure the continued appropriateness of security measures.

8.2. Continuity and disaster recovery processes are documented and reviewed yearly.

## 9. Security incidents

9.1. Security incidents are managed following the University's information security policy and the UTHPC security incident procedures.

9.2. Security incidents must be handled to minimise the damage that may occur during the incidents.

9.3. The information collected while resolving an incident will be documented and analysed to prevent similar incidents from occurring in the future and to decide on the need for additional security measures.

9.4. If signs of a criminal offence, misdemeanour or disciplinary offence or breach of an employment contract are discovered while resolving a security incident, the case shall be processed to an institution or person entitled to conduct the respective proceedings.

9.5. The security incident handling process and the selection of security measures shall be reviewed annually and/or after each incident identified as having failed or deficiencies in preventing and handling security incidents.

## 10. Emergency

10.1. An emergency is an incident that goes far beyond UTHPC jurisdiction - particularly fire, flood, bomb threat, long-term disruption of core services, or any other significant damage that UTHPC alone cannot be expected to repair.

10.2. The University's fire safety rules, evacuation plans, and other rules governing emergencies will apply in an emergency.

10.3. Recovery from significant physical damage (fire, flood, burglary, etc.) is based on the relevant University guidelines.

10.4. If necessary and possible, UTHPC will provide assistance in resolving the emergency.

10.5. After an emergency, the UTHPC manager organises the restoration of UTHPC working conditions in cooperation with the head of the Institute of

Computer Science, ITO (Information Technology Department of Univeristy ) and other University units.

10.6. When recovering from an emergency, services will be restored in order of priority.

10.7. UTHPC users are temporarily directed to use the resources of UTHPC partners, if possible and necessary.

10.8. If it is not possible to use the UTHPC office premises for work, the work will be continued remotely.

## 11. Back-up

11.1. Back-up ensures that data is preserved during data loss due to failure or human error.

11.2. The UTHPC manager is responsible for organising and operating the backups for UTHPC resources.

11.3. The backup type is incremental, which means only changed information is backed up.

11.4. A tape robot is used for backup, physically located in another location.

11.5. The backup system is located in another Data centre, the backup tapes are not physically removed from the tape robot, except in special cases (eg. data transport, etc,).

11.6. The tape robot database marks the backup data (backup time, files to be backed up, etc.).

11.7. If the data volume of the backup system increases to 80% of the maximum volume, an expansion or replacement of the backup system will be arranged.

11.8. Systems are in an automatic backup process and are backed up every night.

11.9. System logs are backed up along with the backup of the log servers.

11.10. Back-ups are kept under the time limits laid down in the contracts.

11.11. Discarded backup data will be deleted, and the media will be reused.

11.12. A dedicated service provider physically destroys discarded tapes.

11.13. Until destruction, the tapes are kept in the tape robot’s room.

11.14. The data on the tapes will be erased before destruction.

11.15. The operation of the backup system is constantly checked.

11.16. The backup system is monitored internally and by a system independent of the backup server.

## 12. Personnel

12.1. UTHPC will ensure sufficient employees to ensure that services are running and available in the event of planned and unplanned absences.