Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Security Guidelines for the Administration of Computer Systems within Leonhard Med

Table of Contents

1 Scope 2
2 Definitions 2
3 Guidelines 2
1 Delegation of administrative responsibilities to persons outside IT Services of ETH Zurich 2
2 Security of administrator access to the computer system 3
3 Security of the administered computer system 3
4 Security of the services running on the computer system 3

Version History

Version	Historie / Status	Datum	Autor/in
0.1	First Draft	08.10.2018	Bernd RInn
0.2	Feedback from HPC group	17.07.2019	Christian Bolliger
0.3	Define prerequisites for external administrators	21.07.2019	Bernd Rinn
1.0	Final policy	26.08.2019	Bernd Rinn

1 Scope

This document refers to “The Acceptable Use Policy of the Leonhard Med secure High Performance Computing Infrastructure” (AUP).

These guidelines specify requirements for the secure administration of computer systems. It is binding for all computer administrators working within the Leonhard Med computing platform.

2 Definitions

Tenant*:* A Leonhard Med tenant separates research projects and institutional use cases from each other. A tenant consists of separate network space containing access, computing and data resources and protected by its own set of firewall rules.

Secure isolated tenant: A secure tenant is a tenant in Leonhard Med that is used by exactly one research project, research lab or institutional customer and that has a single Project Leader (PL), which is responsible for the use of the tenant.

Secure shared Tenant: A secure shared tenant in Leonhard Med is a tenant used jointly by multiple research projects, research labs, or institutional customers. A secure shared tenant does not have a single Principal Leader who is accountable for the use of the *tenant*.

3 Guidelines

1 Delegation of administrative responsibilities to persons outside IT Services of ETH Zurich

Scientific IT Services (ETH Zurich) operates Leonhard Med and is responsible for the secure system administration of the platform and its services. Under certain conditions, Scientific IT Services can delegate the system administration of a Virtual Machine (VM) running within the Leonhard Med platform to administrators outside of IT Services:

- The VM is part of a secure isolated tenant of Leonhard Med.
- When the PL of the secure isolated tenant wishes to pass over administration of the VM to a third party she/he shall aim that request in writing to ETH Scientific IT Services. She/he shall take accountability for the actions of said third party. The designated administrator needs to be named in person.
- The designated administrator must have a good track record of securely administrating server computer systems.
- The designated administrator must sign a declaration that he or she has read and accepts the “ ETH Zurich Acceptable Use Policy for Information and Communications Technology (“BOT”), the “Leonhard Med Acceptable Use Policy (AUP)”, “Guidelines for the Administration of Computer Systems within LeonhardMed” and this document, and shall comply with them.

2 Security of administrator access to the computer system

Access to computer systems (login nodes, virtual machines, and other types of computing systems) has to use the SSH protocol.

Password authentication must be disabled and replaced with private/public SSH key pairs.

Private SSH keys must be encrypted and protected by a passphrase. The latter must follow the ETH password policy.

Preconfigured guest accounts on the VM must be disabled. The minimum set of user accounts required for proper operation shall be configured on the VM.

Privileged administration accounts with elevated permissions must be distinct from the regular ETH user account of any of the administrators.

3 Security of the administered computer system

The operating system must be under security support by its vendor or publisher.

All security features of the operating system shall be used. Contact IT Services if exceptions are required.

Security patches must be installed as soon as they become available. To this end, the operating system shall be configured to download and apply security patches automatically.

The system administrator must check weekly if the patches have been applied, and apply them manually if needed.

Applications that are not patched automatically must be manually updated on a regular basis, and immediately if they are subject to known vulnerabilities.

Only software from well-known, safe sources may be installed. This can be software signed by the OS vendor or software known to the user or system administrator, such as specific scientific software.

Event logging must be activated. Logs shall be forwarded to a central repository if provided by IT Services. Logs shall be kept for at least 6 months.

4 Security of the services running on the computer system

Only required services must be running on the system. All services enabled in the default installation of the operating system have to be checked in this regard.

Required services running on the system are only accessible from within Leonhard Med. Network tunnels to make these services accessible from outside Leonhard Med are not permitted, except for computers or domains white-listed by IT Services.