Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Security Guidelines for ETH Zurich Leonhard Med Endpoints

Table of Contents

Version History

Version	Historie / Status	Datum	Autor/in
0.1	First Draft	08.10.2018	Christian Bolliger
0.2	Second Draft	30.10.2018	Anja Harder
0.8	Third Draft	13.11.2018	Anja Harder / Bernd Rinn
0.9	Pre-final Version	16.11.2018	Bernd Rinn
0.9.1	Corrections from G. Rätsch, N. Toussaint	30.1.2019	Anja Harder, Bernd Rinn, Rui Brandao
1.0	Final Version	21.02.2019	Bernd Rinn

1. General

1.1. Scope

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

These guidelines specify requirements for the secure setup, maintenance and use of computer systems, which are used as an "Endpoint" to Leonhard Med. This document uses the term "Endpoint" as defined by Art. 2(5) as a computerized device connected to Leonhard Med by a network. This guideline is mandatory for members of ETH Zurich and serves as reference for other institutions.

2. Guidelines

2.1. Secure the user accounts on the endpoint

- Accessing an Endpoint (e.g., login into the Endpoint or the Endpoint coming back from sleep or lock mode) must be protected by password, by biometric method or by access token. The use of automatic login features is prohibited.
- Passwords must follow the ETH password policy.[1] Default passwords of preconfigured accounts must be changed.
- Administrator accounts (Windows) or root-accounts (linux/unix, Mac OS)must not be used for regular tasks. In particular, do not use these accounts to read email and to surf the internet.
  That means that a regular user account has to be created after installation of a new operating system if such account does not yet exist. This regular user account should serve as your default account. Use the administrator account only to manage the Endpoint.
- Preconfigured guest accounts must be disabled.
- It is recommended to rename preconfigured administrator accounts (e.g., Administrator in Windows) if possible.

2.2. Protect from illegitimate local access

If an Endpoint is located inside a data center, the location of the Endpoint must be protected with strong physical access control.

For Endpoints not located in a data center, the following regulations apply:

- The premises where the Endpoint is located must be locked when unattended.

[1] See NETHZ Admin-Tool, "Passort ändern": https://idn.ethz.ch/cgi-bin/admin_tool/main.cgi

- It is strongly recommended to encrypt the Endpoint's hard disk or at the minimum the User's home directory.
- It is strongly recommended to protect the Endpoint's BIOS or Firmware with a password.

2.3. Configure your system securely

- Security patches must be installed on the Endpoint as soon as they become available and where applicable are released by the IT Services or the departmental IT support group. To this end, set the update function on your system so that updates are downloaded automatically and preferably being installed automatically. Check weekly, if the patches have been applied and check also if applications that are not automatically patched need to be updated manually. Managed clients using managed software only are considered safe in this regard.
- Event logging must not be deactivated on an Endpoint. On server systems, logs should be forwarded to a central loghost if provided by the organization. Logs should be kept for at least 6 months.
- Stop automatic file sharing mechanism systems (such as NetBIOS). Enable file sharing server software like CIFS and NFS only on server systems and only when needed.
- It is recommended to disable Bluetooth and WLAN if not needed.

2.4. Use the software security features of your operating system

- All security features of your OS recommended by the vendor should be used. Contact IT Services if exceptions are required.
- If your Endpoint is not a server system located in a protected network zone, the local software firewall of your system must be enabled. Do not allow incoming traffic unless you need remote access (such as Secure Shell [SSH] or Remote Desktop Protocol [RDP]) to your system. In such case, configure the local software firewall specifically to allow incoming connections to the remote access software you are using. IT Services or the departmental IT support group can provide help if needed.
- The Endpoint must be protected against malware. This can be done by using a malware detection software, such as a virus scanner. The use of a virus scanner in general is highly recommended. ETH users can use the virus scanners provided on the ETH IT-Shop (https://idesnx.ethz.ch/).

2.5. Use your system securely

- For a personal Endpoint (e.g., Desktop, Laptop, Tablet), the screen must be locked when the User is away from his or her keyboard. To this end, invoke the screen lock manually when you leave your desk.
- Use VPN when you are connected over WLAN. You can use the VPN of ETH Zurich.
- On the Endpoint, only software from well-known, safe sources must be installed. This can be software signed by the OS vendor or software well known to the user or system administrator of the Endpoint, such as specific scientific software. Managed clients (from

IT Services or departmental IT Support Groups) using managed software are considered safe in this regard.

- The version of the operating system (OS) being used must be under security support by the vendor or publisher.

2.6. Protect the ssh-key and user credentials related to the access to Leonhard Med

- Private ssh-keys related to the access to Leonhard Med must be encrypted. The password protecting the key must follow the ETH password policy.
- Private ssh-keys should not be sent over a network or put on an external storage device (e.g., an USB key). If this cannot be avoided, the network must be encrypted and the private ssh-key must be protected by an additional Encryption on User Level, e.g., using GNU Privacy Guard.
- Backups of ssh-keys related to the access to Leonhard Med must be encrypted on the media. If no encrypted backup method is available, restrain from backing up those ssh-keys.
- The one-time password (OTP) secret related to accessing Leonhard Med must not be stored on the Endpoint. Encrypted back-ups of the OTP secret on the Endpoint (e.g. keychains) are acceptable.
- No clear text access credentials such as passwords or passphrases, neither related to Leonhard Med nor to the Endpoint itself, must be stored on any digital or analog device or storage media.