Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Acceptable Use Policy (AUP)

of the Leonhard Med secure High Performance Computing Infrastructure

---

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Acceptable Use Policy of the Leonhard Med High Performance Computing Platform

Based on article 11b paragraph 3 Sub-paragraph d of the Organisational Ordinance of ETH Zurich of 16 December 2003[1] *and the decree of the Executive Board from September 6, 2016 (SLB 06.09.16-06.06),*

the Vice President for Research and Corporate Relationship (VPFW) and the Vice President for Human Resources and Infrastructure (VPPR) enact the following Usage Regulation:

[1] Organisational Ordinance of ETH Zurich (RSETHZ 201.021).

Section 1. General Provisions

Art. 1 Purpose of Policy

The purpose of this policy is to prevent breach of confidentiality, integrity, or availability of sensitive Personal Data, or other confidential research data, entrusted to the "Leonhard Med IT" system. Leonhard Med is a high-performance IT platform provided by ETH Zurich IT Services ("ETH IT Services") to securely store, manage, compute on and share confidential research data.

Art. 2 Definitions

[1] Definitions in article 2 Acceptable Use Policy for Telematics Resources (BOT)[2] are part of this policy. Some of the definitions are narrowed to meet the requirements of systems designed for processing of confidential data.

[2] The term "*User*" includes all persons who are authorized to use the systems governed by this policy. This includes members of ETH Zurich as well as other institutions, independent of their affiliation, work contract and location. Users can be represented by the head of their research group.

[3] The term "*Project Leader (PL)*" denotes the person responsible for organizing a research project on Leonhard Med and leading it scientifically.

[4] All IT systems part of the Leonhard Med platform are denoted by "*System*" or "*Systems*" within this policy.

[5] The term "*Endpoint*" refers to a computerized device connected to Leonhard Med by a network. Examples are a Secure Compute Service in a partner institution, a notebook computer of a user, or the control computer of a scientific measurement device.

[6] "*Public data*" is any data that has been approved for publication by the relevant authority (e.g. PL, Executive Board or Corporate Communications). All data is deemed to be internal or confidential unless or until such approval has been granted.

[7] "*Internal Data*" in the context of this policy means information intended for members of ETH Zurich, or for all project partners of a project using Leonhard Med.

[8] The term "*Confidential Data*" must be used as defined by the "Directive on Information Security at ETH Zurich" [3]. In particular, here we refer to "*Confidential Data*" as including, but not restricted to, all personal data (either identifying or pseudonymized data, in particular health-related or medical data) unless explicitly classified differently. The access to confidential data must be restricted only to those parties with rightful and legitimate access

[2] Acceptable Use Policy for Telematics Resources (BOT; RSETHZ 203.21).

[3] Directive on Information Security at ETH Zurich (RSETHZ 203.25en).

to Leonhard Med. The impact of such data leaking to parties without rightful and legitimate use or to the public may cause major harm to the person from whom the data originate, to the original Data Provider (Controller), to the research organization, or to ETH Zurich.

[9] The term "*Personal Data*" refers to any information related to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In general, Personal Data are regarded as Confidential Data unless explicitly classified differently.

[10] The term "*Data Controller*" means the natural or legal person, public authority, agency or other body that decides on the purpose and means of the processing of Personal Data. Within the scope of this policy, the data controller is either ETH Zurich or a partner institution, which contractually mandates ETH Zurich to process Personal Data.

[11] The term "*Encryption*" in the context of this Acceptable Use Policy Leonhard Med (AUP) means usage of cryptographic methods to make data only accessible to legitimated Users in possession of a cryptographic key and/or a secret.

[12] The term "*Encryption on User Level*" refers to an Encryption process, which is under the full control of the User. This implies that the User is in charge of encrypting and decrypting the data, managing the encryption keys and selecting the appropriate encryption method.

[13] The term "*Shared Data Set*" refers to reference data sets shared with the scientific community at large. An example is the Cancer Genome Atlas shared by NIH.

Art. 3 Scope of Policy

[1] The Acceptable Use Policy Leonhard Med (AUP) applies to any use, whether by ETH Zurich members or third parties, of the Leonhard Med data platform provided by ETH Zurich.

[2] The IT security of all Systems, which are part of the Leonhard Med platform, and all Endpoints, with regard to their function as an Endpoint of Leonhard Med, are within the scope of this policy.

Section 2. Use

Art. 4 Purpose and scope of use

[1] The purpose of Leonhard Med is mainly to store and process data for research projects that require storing and processing of Confidential Data as well as of other data. Examples are health-related personal research data. Priority is given to projects which need to process Confidential Data.

[2] The security level of the System is designed for storing, maintaining and processing Confidential Data. At the system level, these standards remain the same for all projects.

[3] Under this AUP, Leonhard Med may be used for research and teaching. For other use cases e.g. for clinical decision support, amending agreements are required.

Art. 5 No Private Use

Private use of the System is prohibited.

Art. 6 Data Classification

[1] Data classes and the process of data classification is defined in the "Directive on Information Security at ETH Zurich" [4]. Definitions of data classification have been adapted to the purpose of Leonhard Med and are listed in Art. 2.

[2] For the responsibility of data classification, see article 9 paragraph 8.

[3] All Personal Data are classified as Confidential Data unless explicitly classified differently and except the ones listed in article 6 paragraph 4.

[4] Personal data identifying the Users of the Systems, e.g. name, email address or affiliation, are classified as "Internal".

Art. 7 Processing of Confidential Data

[1] The user represents and warrants that all legal, contractual and ethical requirements for processing confidential data are fulfilled and the data she/he supplies have been lawfully obtained and can be lawfully processed.

[2] Only Encrypted data transfer protocols are permitted for transfer of Confidential Data, unless the source does not technically support encrypted protocols.

[3] Data Transfer of Confidential Data into and out of the System must be Encrypted on User Level, except in the following cases:

[4] Directive on Information Security at ETH Zurich (RSETHZ 203.25en)

A. *Shared Data Set*: Transfer of a Shared Data Set from a white-listed organization (cf. article 13).

B. Sender is Recipient: Transfer of a data set when all of the following conditions are fulfilled: a) the User initiating the transfer is both sender and recipient, b) the data transfer is between a secure network (e.g., from a Leonhard Med project partner) and Leonhard Med.

C. Data *Transfer from Individuals:* Data sent from an individual who consented to provide his or her data, if the sender device does not technically support Encryption on User Level.

Section 3. Accountability and Responsibility

Art. 8 Responsibility of the User

[1] The user shall be personally responsible for ensuring that her/his use of the telematics resources does not violate the provisions of this Acceptable Use Policy or of the applicable laws (e.g., criminal law, data protection regulations, human research act), or infringe third party rights (e.g., personal rights, privacy, copyrights, license terms). The user is namely responsible to treat confidential data accordingly

[2] The User shall be responsible for the confidentiality of personal access data und identification mechanisms, such as passwords, PINs, private keys, chip cards, physical keys, tokens. The Users may not disclose or make available this access data to third persons, or give them access under their account name.

[3] The obligation to maintain confidentiality is not limited in time and persists.

[4] The User represents and warrants that all legal, contractual and ethical requirements for processing medical research data are fulfilled. The User is liable for any unlawfulness, any negligence or any infringements of this policy.

[5] All Leonhard Med users are responsible to comply with the rules laid down in the "ETH Zurich Acceptable Use Policy for Telematics Resources" (BOT). In addition, users must comply to the rules laid down in their specific collaboration agreement with ETH Zurich.

Art. 9 Responsibility and Accountability of the Project Leader (PL)

[1] The Project Leader (PL) is accountable for the legally and ethically correct handling of all Confidential Data of a research project. He/she must ensure that all data in her/his research projects have been lawfully obtained and are lawfully handled according to this regulation and all other applicable laws, guidelines and policies.

[2] The PL is responsible for the whole project data lifecycle within Leonhard Med.

[3] Any contractual requirement for technical data protection beyond the measures listed in Section 4 "Security Measures" is in the accountability of the PL. This may include data Encryption on User Level.

[4] The PL of a project represents the data controller towards ETH IT Services. He or she is accountable for all legal and contractual obligations within the scope of his/her project.

[5] The PL ensures he/she has a copy of all documents regulating data processing and privacy within a project that he/she can provide to the Chief Information Security Officer (CISO) or ETH IT Services on request. This includes the data transfer agreements, specific policy regulations, the authorisation by the ethics committee and other regulatory decisions. The current list will be provided by ETH IT Services every three months.

[6] The PL, or a person designated by the PL ("responsible person"), names the persons who are entitled to access and process sensitive data of his/her project. The responsible person revises the list of persons with access rights to the data of a research project at least twice per year and provides the revised list to ETH IT Services. The current list will be provided by ETH IT Services every three months.

[7] The PL ensures that all persons with access rights to the data of the project have signed an agreement stating that they will follow the Leonhard Med AUP.

[8] The PL is responsible and accountable for the correct data classification within his/her project as defined in Art. 2.

[9] The PL is accountable for the security of the Endpoints accessing data in his/her project.

[10] The PL is responsible for authorising transmission of Confidential Data to Endpoints, considering rules defined by the ETH IT services department of his/hers organization where applicable.

Art. 10 Responsibilities of ETH IT Services

[1] ETH IT Services is responsible for the secure operation of the Leonhard Med platform and can release further technical policies and regulations to ensure security of the platform and any data stored and maintained on it.

[2] ETH IT Services is responsible for providing and keeping up-to-date "IT Security Guidelines for Leonhard Med Endpoints"[5].

[5] IT Security Guidelines for ETH Zurich Leonhard Med Endpoints (RSETHZ 438.2).

Art. 11 Responsibilities of the ETH Zurich Chief Information Security Officer (CISO)

[1] The CISO can limit or impose further requirements for access to the Leonhard Med platform from certain countries or networks for security reasons.

[2] The CISO can set further requirements for users wanting to access Leonhard Med during travel from certain foreign countries or networks for security reasons.

Section 4. Security Measures

Art. 12 High-Risk Systems

All Systems and all Endpoints ruled by this AUP are systems with a high level of protection according to article 23 Directive on Information Security at ETH Zurich[6].

Art. 13 Access Protection

[1] User access to Leonhard Med requires a two-factor authentication (2FA). The user is required to install the second factor of authentication on an independent Endpoint (e.g. smartphone) or a special device designed for that purpose except for automated access.

[2] ETH IT Services offers 2FA authentication services.

[3] Automated access to the Leonhard Med Systems requires approval by ETH IT Services.

[4] In the event of suspicion that access data or an identification mechanism has been disclosed or made available to a third party, or has been used by a third party, the user must promptly act to report the incident to the system administrators.

[5] The User must promptly report any irregularities they observe while accessing or using the System or the Endpoint to the system administrators.

[6] The User must not circumvent any access protecting mechanism.

Art. 14 Accessing the Internet from the System

[1] Internet access from Leonhard Med is restricted by technical means to a selected subset of sites ("white list"). ETH IT Services chooses the white list to contain only sites where Users need to have access from for Leonhard Med to fulfil its purpose and that do not compromise confidentiality, integrity and availability of data on Leonhard Med. Users can request the addition of sites to the white list. Denial of such a request will be explained.

[6] Directive on Information Security at ETH Zurich (RSETHZ 203.25en).

[2] The User must not circumvent any access restriction.

Art. 15 Endpoints

[1] All users are responsible for ensuring confidentiality and integrity of Confidential Data stored and processed on their endpoints and that their endpoints do not compromise the security of Leonhard Med and the data residing on it.

[2] Endpoints of ETH Zurich users must be setup, administrated and used according to the "IT Security Guidelines for Leonhard Med Endpoints". In particular, User access to an Endpoint has to be protected by strong passwords or equivalent or better access control. Endpoints have to receive frequent software updates and common OS specific security measures must be enabled.

[3] Organizations other than ETH Zurich with access to Leonhard Med may define and enforce their own guidelines or best practices for Endpoint security. The measures described in ETH Zurich's "IT Security Guidelines for Leonhard Med Endpoints" are recommendations for ensuring appropriate security of the organizations' endpoints.

[4] Access keys used in the context of Leonhard Med, e.g. SSH keys, and cryptographic keys to access data must be passphrase protected (at least 12 characters) on all endpoints.

[5] All network traffic between client Endpoints and the Systems must be encrypted.

Art. 16 Logging of User Activity

[1] All User activities on the System may be logged by ETH IT Services. This includes but is not limited to User login, access to compute nodes, data changes, usage of the batch system or attempts of access violation or privilege escalation.

[2] These logs may be used by ETH IT Services to detect successful or attempted breaches, to examine unusual system states and to guarantee the proper function of the System.

[3] ETH IT Services is entitled to provide to a PL usage information about the project's resources, and summary information about the resource usage of each User in the project.

Section 5. Abuse

Art. 17 Abuse

Any infringement of this AUP or unlawful conduct using Leonhard Med is considered an abuse. Abuse will be handled according to article 18 ff. BOT[7] and can imply civil or administrative action or liability, as well as criminal prosecution.

Section 6. Escalation Path

Art. 18 Escalation Path

[1] Non-compliant behaviour with this policy can be escalated by ETH IT Services to the Vice-President of Research and Corporate Relations (VPFW) or the Vice President of Human Resources and Infrastructure (VPPR).

[2] Objections to the applicability of this policy have to be addressed to the Director of ETH IT Services.

[3] The VPFW takes the final decision in case of objections to the decision of the Director of ETH IT Services.

[7] Acceptable Use Policy for Telematics Resources (BOT; RSETHZ 203.21).

Section 7. Final provisions and transitional provisions

Art. 19 Effective date

This regulation will become effective as of May 1st 2019.

Art. 20 Transitional period

All organizations and users covered by this AUP must comply with the rules and regulations provided in this AUP within 6 months after the effective date.

Zürich, May 1st 2019

Swiss Federal Institute of Technology Zurich

Vice President of Research and Corporate Relations
Prof. Dr. D. Günther

Vice President of Human Resources and Infrastructure
Prof. Dr. U. Weidmann