Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

RSETHZ 438.1

The Acceptable Use Policy (AUP)

of the Leonhard Med Secure Scientific IT Platform

of August 1st 2022; Version 2.0

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Acceptable Use Policy of the Leonhard Med Secure Scientific IT 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 (VPF) and the Vice President for Infrastructure (VPIN) 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 strictly confidential and confidential data, or other research data, entrusted to Leonhard Med, as defined in article 2 section 2 of this policy.

Art. 2 Definitions

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

[2] The term "***Leonhard Med***" denotes the secure, versatile and high-performance scientific data and IT platform at ETH Zurich, designed, built and operated by the Scientific IT Services at the IT Services ETH Zurich, for secure transfer, storage, management and computational analysis of strictly confidential and confidential data in research.

[3] 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 are represented by the head of their research group.

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

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

[6] 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.

[7] The terms *"**Information**"* and *"**Data**"* are used here as interchangeable terms.

[8] The term "***Personal data***" refers to any information related to an identified or identifiable natural person as defined in article 3 let. a Federal Act on Data Protection (FADP, SR 235.1)[3]. 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, geolocation 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.

---

[2] Acceptable Use Policy for Information and Communications Technology (BOT; RSETHZ 203.21).

[3] Federal Act on Data Protection (FADP): https://fedlex.data.admin.ch/eli/cc/1993/1945_1945_1945

[9] ***"Classification of information"*** refers to classification of information or data according to their confidentiality level — public, internal, confidential or strictly confidential — as defined in Articles 20 - 22 of the ETH Directive on Information Security at ETH[6].

[10] The term ***"strictly confidential information"*** must be used as defined by art. 22 sec. 1 let. d ETH Directive on Information Security[6]. With regard to data storing or processing within Leonhard Med, strictly confidential data includes but is not limited to: all personal data (either identifying or pseudonymized data, such as health-related or medical data) unless explicitly classified differently.

In particular:

- information that identifies individuals directly (e.g. tables storing the identity information of a person mapped to a corresponding unique code, used for de-identification by means of coding - here, referred to as "pseudonymisation") shall be classified as strictly confidential data,
- health-related or medical data represented in coded form (here, referred to as "pseudonymized") are subject to the Human Research Act[4] and shall be classified as strictly confidential data.

Exception to these and therefore open to lower confidentiality classification, are health-related or medical data that have been irreversibly anonymised in accordance with article 25 Human Research Ordinance[5] or explicitly given a different classification (see "Classification of information" definition).

The access to strictly confidential data entrusted to Leonhard Med must be restricted only to those parties with rightful and legitimate access authorization. The impact of such data becoming accessible to parties without rightful and legitimate use or to the public may cause major harm to the person from whom the data originate, or severely damage the interests of ETH Zurich, data controllers or research organizations.

[11] The term ***"confidential information"*** must be used as defined by art. 22 sec. 1 let. c ETH Directive on Information Security[6]. With regard to data storing or processing within Leonhard Med, confidential data includes but is not limited to: all personal research data that are **not** subject to the Human Research Act[4].

In particular:

- personal data of a particularly sensitive nature and personality profiles in accordance with Article 3 of the Federal Act on Data Protection may be classified as confidential data, except for health-related or medical data that are subject to the Human Research Act[4] and which shall be classified as strictly confidential data (cf. paragraph 10 above).

[4] Human Research Act (HRA): https://fedlex.data.admin.ch/eli/cc/2013/617

[5] Human Research Ordinance (HRO): https://fedlex.data.admin.ch/eli/cc/2013/642

The access to confidential data entrusted to Leonhard Med, must be restricted only to those parties with rightful and legitimate access authorization. The impact confidential data becoming accessible to parties without rightful and legitimate use or to the public may cause significant harm to the person from whom the data originate, or significantly damage the interests of ETH Zurich, data controllers or research organizations.

[12] "***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.

[13] **"*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, confidential or strictly confidential unless or until such approval for publication has been granted.

[14] The term "***Data Controller***" represents the natural or legal person, public authority, agency or other body that decides on the purpose and means of the processing of data (in particular but not limited to, strictly confidential or confidential data). Within the scope of this policy, the data controller is either an institution, which provides the data and which contractually mandates ETH Zurich to process data, or possibly (also) ETH Zurich.

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

[16] 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.

[17] The term "***Shared Data Set***" refers to reference data sets shared with the scientific community at large.

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 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 strictly confidential (such as health-related or medical data) and confidential data as well as of other data. Priority is given to projects which need to process strictly confidential and confidential data.

[2] The security level of the System is designed for secure transfer, storage, management and computational analysis of such data. At the system level, the standard security controls that ensure the very high level of protection remain the same for all uses of Leonhard Med (e.g. strictly confidential and confidential data). Accordingly, all technical and operational measures of Leonhard Med are compulsory for strictly confidential and confidential data and remain the same when handling other classes of data (i.e., internal, public) in Leonhard Med.

[3] The regulations in this policy are compulsory for strictly confidential data and for confidential data.

[4] 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"[6]. This data classification has been applied and further specified to the purpose of Leonhard Med as is stipulated in article 2 of this AUP.

[2] The PL is responsible for correct data classification according to article 9 of this AUP.

[3] In general, personal data are classified as either strictly confidential or as confidential data unless explicitly classified differently and except the ones listed in article 6 paragraph 4 of this AUP.

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

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

Art. 7 Processing of Strictly Confidential and Confidential Data

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

[2] Only Encrypted data transfer protocols are permitted for transfer of strictly confidential and confidential data unless the source does not technically support encrypted protocols.

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

A. *Shared Data Set*: Transfer of a Shared Data Set from a white-listed organization (cf. article 2 paragraph 17 of this AUP).

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 trusted secure network (e.g. white-listed research institution, hospital) and Leonhard Med.

C. Data *Transfer from Individuals:* Data sent from an individual person who consented to provide their 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 Users shall be personally responsible for ensuring that their use of the information and communications technology do 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 Users are namely responsible to treat strictly confidential data and confidential data in compliance with this AUP and all other applicable regulations (e.g. laws, policies, guidelines).

[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 strictly confidential and confidential data are fulfilled. The User is liable for any unlawfulness, any negligence or any infringements of this AUP.

[5] The Users are responsible to comply with the rules laid down in the "ETH Zurich Acceptable Use Policy for Information and Communications Technology " (BOT). In addition, Users must comply to the rules laid down in their specific agreement with ETH Zurich (e.g. Collaboration-, Research-, Project Agreement).

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 strictly confidential and confidential data of a research project. PLs must ensure that all data in their research projects have been lawfully obtained and are lawfully handled according to this AUP and all other applicable regulations (e.g. laws, policies, guidelines).

[2] PLs are responsible and accountable for the data that has been collected and processed by them or on their behalf and that they entrust to Leonhard Med, within the scope of a research project or any other use of data at Leonhard Med. PLs are 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" of this AUP 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 shall provide to the Chief Information Security Officer (CISO), Data Protection Officer (DPO) or IT Services of ETH on request (“Data Protection Documentation”). This includes the data transfer agreements, specific policy regulations, the authorisation by the ethics committee and other regulatory decisions.

[6] PLs, or a person designated by the PL ("Permissions Manager"), shall name the persons who are entitled to access and process strictly confidential and confidential data of his/her projects. That list of persons shall be updated at least twice per year and shall be provided to ETH IT Services without being prompted.

[7] The PL ensures: (i) that all Users (including PLs and persons with access rights to the data of the project) have signed an agreement stating that they will follow the Leonhard Med AUP and (ii) that all Users have followed trainings in data security and privacy before accessing strictly confidential or confidential data in Leonhard Med.

[8] The PL is responsible and accountable for the correct data classification within his/her project as defined in article 2 paragraph 9 of this AUP.

[9] The PL is accountable for the security of the Endpoints accessing data in his/her project, according to the "IT Security Guidelines for Leonhard Med Endpoints"[7].

[10] The PL is responsible for authorising transmission of strictly confidential and confidential data to Endpoints, considering rules defined by the ETH IT services department of his/her 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, managed and processed on it.

[2] ETH IT Services is responsible for providing and keeping up-to-date "IT Security Guidelines for Leonhard Med Endpoints"[8].

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

[1] ETH Zurich's 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 Systems with very high level of protection

All Systems ruled by this AUP have a very 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 two-factor authentication (2FA) services.

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

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

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

[4] In the event of suspicion that User 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 Service Desk of Leonhard Med (leomed-support@id.ethz.ch) or of ETH IT Services (servicedesk@id.ethz.ch).

[5] In the event of an information security incident concerning Leonhard Med (e.g. data breach affecting personal data or pseudonymised/ coded data) the User or PL must immediately inform the Service Desk of Leonhard Med (leomed-support@id.ethz.ch) or of ETH IT Services (servicedesk@id.ethz.ch) and ETH Zurich's Data Protection Officer (DPO) and CISO. Outside office hours, the ETH Zurich Emergency Desk is available in case of emergencies per phone at +41 44 342 11 88.

[6] The User must promptly report any irregularities they observe while accessing or using the System or the Endpoint to the Service Desk of Leonhard Med (leomed-support@id.ethz.ch) or of ETH IT Services (servicedesk@id.ethz.ch).

[7] 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 by ETH Zurich of such a request will be explained but can not be contested.

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

Art. 15 Endpoints

[1] All Users are responsible for ensuring confidentiality and integrity of strictly confidential and confidential data stored and processed on their Endpoints. Users are responsible 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"[8]. In particular, User access to an Endpoint has to be protected by strong passwords or equivalent or better access control, according to the current state-of-the art technologies. Endpoints have to receive frequent software updates. Common Operating System (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"[8] represent a minimum standard 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[9] 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 AUP can be escalated by ETH IT Services to the Vice President for Research (VPF) or the Vice President for Infrastructure (VPIN).

[9] Acceptable Use Policy for Information and Communications Technology (BOT; RSETHZ 203.21en).

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

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

Section 7. Final provisions and transitional provisions

Art. 19 Effective date

This regulation will become effective as of August 1st 2022.

Art. 20 Transitional period

Within 6 months (February 1st 2023) after the effective date, the PLs are responsible to ensure that new and existing data of their projects at Leonhard Med are correctly classified (e.g. strictly confidential or confidential) as per regulation defined in this AUP and in compliance with the Directive on “Information Security at ETH Zurich” (RSETHZ 203.25).

Zürich, August 1st 2022.

Swiss Federal Institute of Technology Zurich

Vice President for Research
Prof. Dr. D. Günther

Vice President for Infrastructure
Prof. Dr. U. Weidmann