Information Systems Security Policy LEX 6.5.1

2nd June 2014, status as at h 1st January 2025

The Direction of the Ecole polytechnique fédérale de Lausanne
Based on the Federal Act on the Federal Institutes of Technology (ETH Act);
Based Arts. 57i et seq. of the Government and Administration Organisation Act (GAOA);
Based on the Ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération;
Based on Art. 3, para. 1, letter a of the Ordonnance du Conseil des EPF sur les écoles polytechniques fédérales de Zurich et de Lausanne (Ordonnance sur l'EPFZ et l'EPFL);
Based on Ordinance on the Organisation of the Ecole polytechnique fédérale de Lausanne, in particular Arts. 4 and 13;
Based on Loi fédérale du 24 mars 2000 sur le personnel de la confédération (LPers);
Based on the Ordonnance du Conseil des EPF sur le personnel du domaine des écoles polytechniques fédérales (OPers-EPF);
Based on the Ordonnance de l'EPFL sur les mesures disciplinaires;
Based on the Ordinance for the Use of Software Subject to a License Agreement (LEX 6.1.5) ;
Based on the Directive concerning collective emails (LEX 6.3.3);

hereby adopts the following:

Preamble

This document affects all users of EPFL information systems (hereinafter the information system), regardless of the communication channels used to access the information system, as well as any information created by EPFL or entrusted to it and removed from the scope of the information system.

This evolutionary policy will be adapted to comply with the directives of EPFL, the ETH Board and the Confederation.

Section 1 General Background

Article 1 Scope of the information system

[1] The EPFL information system is considered as a unit consisting of components of various natures and origins, centred on the needs of users. It includes the following main components:

1. infrastructure and equipment available to users individually or collectively;
2. data and data processing;
3. documentation;
4. users and IT staff.

[2] Its scope includes all above-mentioned components owned or leased by EPFL, on all sites, regardless of the means of access to the component. In addition to the information created by EPFL, the scope also includes information entrusted to it by third parties.

Article 2 Importance of information security at EPFL

[1] The EPFL information system is one of its key assets contributing to its objectives.

[2] The growth in needs, number of interconnections and interdependencies, complexity and diversity of systems and threats, contributes to a rapid increase in risks faced by the EPFL.

[3] The security of the EPFL information system - namely its availability, integrity, confidentiality and traceability - must be given special attention. It aims to ensure the continuation of EPFL activities

and to protect the School's reputation in connection with the use of information and resources supporting these.

[4] The EPFL Direction acknowledges the importance of protecting this asset and actively supports the Information System Security Policy (PSSI).

[5] The Director of the Information Systems Management department is responsible for implementing the Information System Security Policy.

[6] The Head of information system security is in charge of managing any security-related crises for such systems, in addition to his/her responsibilities directly related to information security.

Section 2 Foundations & Principles

The Information System Security Policy is based on **pillars** which are equally important as described in the following articles.

Article 3 Pillar 1

The information system is a key asset to EPFL. In this sense, there must be safeguards to protect its value and in relation to the assessment of risks inherent in its unavailability, loss, alteration or theft.

Article 4 Pillar 2

EPFL retains ownership of any of its information removed, with or without its consent, from the scope of its information system. The PSSI - in particular Articles 6 and 18 of this policy - remains applicable.

Article 5 Pillar 3

Any sensitive information is subject to a specific classification.

Article 6 Pillar 4

Except for a change in classification, the level of protection of information against unauthorised access remains the same throughout its life cycle, regardless of its medium (confidentiality and integrity).

Article 7 Pillar 5

Information and its processing are subject to protective measures commensurate with their value against intentional or unintentional unauthorised alterations (integrity).

Article 8 Pillar 6

The level of protection of the information system is adapted globally or locally depending on the value / sensitivity of the information it stores and processes. Such adaptation is documented.

Article 9 Pillar 7

Users of the information system are authenticated and authorised prior to access (authentication and authorisation). Access is tracked and kept out of reach of the users (traceability) to enable identification of any perpetrators of criminal acts. Access logs are accessible to the extent foreseen by the law.

Article 10 Pillar 8

Information needed is available to the users at the appropriate time (availability).

Article 11 Pillar 9

Users have access only to the information they need in their work (need-to-know). Similarly, they perform actions in the information system only to the extent corresponding to their work (need-to-do).

Article 12 Pillar 10

Modifications of sensitive information may be assigned to a given user (traceability). User identification ensures the validity of protective measures.

Article 13 Pillar 11

Financial information is processed according to the principle of separation of duties to prevent fraud and errors (four eyes).

Article 14 Pillar 12

Physical access to sensitive IT media is kept to a minimum and restricted to authorised and identified persons according to the need-to-know and need-to-do principles. Access is tracked. Access logs are accessible to the extent foreseen by the law.

Article 15 Pillar 13

Controls are implemented to prevent or correct incidents and ensure compliance with this policy.

Article 16 Pillar 14

Each user of the information system is individually responsible for the proper use of resources and the protection of information made available by EPFL, with due regard to the interests of EPFL and in compliance with applicable laws, regulations, directives and this policy.

Article 17 Pillar 15

Information security is taken into account in each project involving IT resources and throughout the life cycle of the information system.

Section 3 Stakeholders

Article 18 Responsibilities

[1] All stakeholders are responsible for protecting the information system. Through their behaviour, individual users can either improve such protection or put the system at risk.

[2] EPFL ensures that its employees, students, guests and service providers have efficient resources available in relation to their needs. EPFL also provides training to its staff. In exchange, EPFL expects all users to:

1. protect the EPFL's reputation;
2. avoid exposing EPFL to risks - especially financial, legal or operational - beyond the limits laid down by the institution;
3. take, within the framework set by the EPFL, all necessary measures to protect the information system put at their disposal for their work;
4. immediately notify the relevant bodies of any breach of information system security;
5. preserve the secrecy of any security flaws vis-à-vis unauthorised third parties;
6. use the resources at their disposal to carry out the tasks entrusted to them under their contractual relationship with EPFL;
7. protect any information which they remove from the scope of the information system or which they access from outside the scope of the system.

Section 4 Entry into Force

Article 19 Entry into force

[1] This policy entered into force on 2nd June 2014 and was revised on 15.03.2021 (version 1.2) and on 1st January 2025 (version 1.3).

On behalf of the EPFL Direction:

Anna Fontcuberta i Morral
President

Françoise Chardonnens
Director of Legal Affairs

Annexe: Glossary

Glossary

Accountability	Ability to assign responsibility for an action to an individual.
Asset	Any item of value to the organisation.
Authentication	Process to verify the identity of a user.
Authenticity	The property of being genuine.
Authorisation	Process of granting access privileges to a user.
Availability	The property of being accessible and useable upon demand by an authorised entity.
Classification	Process of assigning a level of sensitivity to information according to its desired level of protection, e.g. public, internal use only, confidential (wages, industrial contracts) or secret (staff member's state of health, assessments by the Academic Promotion Committee).
Cloud Computing	Use of storage and computing capabilities of remote computers and servers via the Internet.
Confidentiality	The property that information is not made accessible or disclosed to unauthorised individuals, entities or processes.
Data	Representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by humans or by automatic means.
Data Owner	Entity or person who authorises or denies access to these data, and is responsible for their accuracy, integrity and timeliness, and sets their classification.
Information	Facts and knowledge derived from data.
Information Security	Protection of confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability may also be involved.
Information System	An information system (IS) is a set of information resources organised for the collection, classification, processing and dissemination of information on a given phenomenon. The use of computer, electronic and telecommunication resources serves to automate and computerise operations such as company procedures. They are now widely used instead of conventional means such as paper forms and the telephone, and this transformation is the origin of the concept of information system.
Integrity	Assurance that information is authentic and complete.
Need-to-do	Principle according to which the users of an information system can interact with the system only as defined in the framework of their official duties. This is sometimes called the principle of least or minimal privilege or of least authority.
Need-to-know	Principle according to which the users of an information system only have access to information they need as part of their work.
Non-repudiation	Assurance that the content of a document or transaction cannot be subsequently challenged.

Reliability	Probability that a component or a complete system will operate without failure for a specified period of time, under specified operating conditions.
Sensitive Information	Confidential information or information whose alteration, whether voluntary or involuntary, whether authorised or unauthorised, may lead to financial loss to the EPFL (e.g. data transmitted to a bank to make a transfer between accounts).
System Owner	Entity or person who authorises or denies access to the system. It ensures: 1. accuracy of the items input into the system 2. accuracy of the system output, 3. system integrity 4. and that the system is up-to-date.
Traceability	Ability to keep track of information through various stages of processing.