l'X

ÉCOLE
POLYTECHNIQUE
UNIVERSITÉ PARIS-SACLAY

Information and communication system user charter

approved by the Health, safety and working conditions committee
on 23 June 2017
approved by the establishment's technical Committee
on 5 July 2017

ARTICLE 1 : INTRODUCTION

The purpose of this charter, drafted in the context of the Information Systems Security Policy (ISSP) of the École polytechnique, is to inform the user of the principles of access to the information and communication system of the École polytechnique, as well as the applicable information system security concepts.

ARTICLE 2 : SCOPE

These provisions concern the use of the digital resources of the École polytechnique, as well as any external digital resources that may be accessed from the École polytechnique: data, software, materials, user names, domain names, internal or external third-party computer systems and subject to the provisions set out by these organisations.

They apply:

- to the staff paid by the École polytechnique (including paid and unpaid interns);
- to the staff not paid by the École polytechnique, who work or are hosted on the premises;
- to the students (engineering school, Bachelor, Graduate Degree, Master's, PhD students and other learners);
- and generally, to any legal or natural person present on the site of the École polytechnique for any reason (visitors, position candidates, workers, unregistered students, staff from external organisations, service providers, guests, volunteers, members of associations, etc.).

The legal framework prevails with regard to the implementation of the rules of this charter. In the event of a contradiction between several regulatory texts (example: security policy, criminal code, telecommunications regulation), only the highest level framework applies.

The École polytechnique, which benefits, among other things, from access to the Internet via the RENATER network, has adopted the RENATER code of ethics[1] dedicated to this access. This charter, as well as the list of all of the digital services offered by the ISD, is available on the ISD website.

The resource access agreement of the Drahi X-novation Center supplements this charter, when relevant.

Any action that violates the provisions of this charter may result in a temporary or permanent suspension of the rights to access the information and communication system, and according to the severity of the violation, may give rise to disciplinary, civil or criminal sanctions.

This charter is appended to the internal regulation of the École polytechnique. Acceptance of the internal regulation automatically implies acceptance of this charter.

ARTICLE 3 : DEFINITIONS

Section 3.1 Digital resources

The term "digital resources" refers to the data belonging to the École polytechnique or entrusted to the École or collected by the École; the IT or telephone equipment; the storage, archiving or back-up equipment; the calculation or management tools; the rights to use the software packages granted to the École; as well as those to which remote-access is possible, directly or through a chain, from the networks administered by the École polytechnique.

For the purposes of the implementation of the rules set out in this charter, any third-party equipment, that may be private, used to access the digital resources of the École becomes a digital resource of the École for the duration of this use.

Section 3.2 Digital services

The term “digital services" corresponds to the provision of information capture, exchange, transformation and/or publication methods by the internal or external digital resources.

Section 3.3 Users

The persons that use or have physical or logical access to the digital resources and the digital services are referred to as "users". They are broken down into the categories described in article 2.

Section 3.4 Information and communication system administrators

The term "information and communication system administrator" refers to any user specifically responsible[1] for the correct operation and the security of the digital resources [2]that form part of the information and communication system.

The information and communication system administrators are divided into two groups, as described below. All the administrators implement the information and communication system security policy of the École polytechnique

Section 3.5 Application administrators

Application administrators are IS (information system) users in charge of operating monitoring activities (processing and data management) linked to an application or a set of applications.

These application administrators are present in all divisions of the École (administration, education, continuing education, entrepreneurship, as well as in the research laboratories).

The application administrators are responsible for the security and the correct operation of the applications under their responsibility.

Some of the application administrators are "application advisors": Application advisors are responsible for setting out the division configuration and configuring the user privileges and profiles.

Section 3.6 System and network administrators

The role of the system and network administrators is to install and technically manage the digital resources of the École polytechnique. These system and network administrators primarily operate within the ISD and sometimes within the management of a division: within the laboratories of the École polytechnique and within the management committee.

The system and network administrators are technically responsible for the security and the correct operation of the digital and telephone infrastructures under their responsibility.

[1] Mission letter, job description, employment contract, service provision contract, etc.

[2] Network equipment, servers, operating systems, applications, etc.

ARTICLE 4 : ACCESS TO THE IT AND TELEPHONE RESOURCES

Section 4.1 Access authorisation for the information and communication system

The use of the IT resources is always based on a division requirement; it is realised by the opening of an account or the right to connect IT or telephone equipment to the network of the École polytechnique.

Section 4.2 Access accountability

This authorisation is strictly personal and therefore under no circumstances may it be transferred to a third party, even temporarily.

The user that holds the authorisation is accountable for the actions carried out through this authorised access.

Section 4.3 Use of resources

The use of the information and communication system is limited to legitimate and legal research, education, technical development, technology transfer, scientific information dissemination, technical and cultural activities, and to any administrative management and support activity linked to these activities.

These resources cannot be used for a purpose external to the École without the prior, formal authorisation of the École polytechnique.

Section 4.4 Cancellation of the access authorisation

The École polytechnique reserves the right to withdraw this authorisation at any time, without notice, due to a proven threat or suspected threat to its information and communication system, and based on the assessment of the CISO or the ISD. The ISD shall make every effort to inform the users affected at the time of such an event.

Section 4.5 Modification and termination of activities

This authorisation ends when the user's activity is terminated and is re-examined at the time of any modification of activity (change of department, change of user category).

In the specific case of students (engineering school students, students from other courses, PhD students), this authorisation ends within a maximum of one year after graduation, unless there are exceptional circumstances, approved by the École polytechnique.

Section 4.6 Closure of access, return of loaned equipment

At the time of the closure or modification of access due to a transfer or departure (examples: LDAP account, file server, application, etc.), the user must provide the École polytechnique and their former department with their professional information.

Prior to their departure, the user is responsible for destroying their private information. Prior to departure, and even in the case of a transfer, a user must return all of the equipment given to them for the performance of their professional activity to their line manager.

Section 4.7 User liability with regard to equipment

In the event of malfunction, breakdown or loss of IT or telephone equipment due to user negligence, payment for the use value of the equipment may be requested.

Section 4.8 École polytechnique email inboxes

Unless explicitly requested from the ISD by the user, and solely in order to redirect emails to an external email address, the École polytechnique email address is deleted at the time of departure from the École polytechnique.

For students (engineering school students, students from other courses, PhD students), this deletion is postponed to five years after departure from the École polytechnique. After departure, a student is free to request the early deletion of their address at any time.

The possession of this email address after the departure of the user requires this party to adhere to this charter with regard to the use of this address.

Section 4.9 Connection of personal equipment to the information and communication system

Any connection of personal equipment to the information and communication system of the École polytechnique is subject to the authorisation of the ISD, and is carried out in accordance with professional use and security rules of the École polytechnique and its laboratories.

The École polytechnique cannot be held liable in the case of theft or damage to the personal equipment of users.

Section 4.10 Reasonable use of the common resources

All users agree to correctly use the resources provided (examples: not to saturate the memory, hard drive, network bandwidth, printers, etc.). For example, email chains or the sending of a large attachment to a mailing list are forbidden.

Section 4.11 Reasonable use of the Internet

Only the Internet services that have a direct and necessary link to the professional activity, as defined in Section 4.3, may be consulted.

Use of the Internet for private reasons is tolerated (example: personal emails, searches outside the professional context, etc.) if it falls within the scope of Section 4.10, if it is one-off and brief, if the content viewed does not violate public order and common decency, and if this use does not unduly interfere with the tasks assigned to the user.

ARTICLE 5 : RESPONSIBILITIES OF THE INFORMATION SYSTEM ADMINISTRATORS

Section 5.1 Assignment of extended rights

Only the administrators have extended rights linked to the role carried out, and not the hierarchical position or job description.

Section 5.2 Duty of confidentiality of administrators

Administrators are bound by a duty of confidentiality in the exercise of their role.

In order to ensure the correct operation and security of the information and communication system, they may carry out the necessary investigations (search for digital evidence, verification of access, technical audit of a computer, etc.).

In order to respond to a legal obligation, the hierarchy may request administrators to provide the information obtained in the exercise of their roles and which falls within the scope of the subject of the obligation.

Section 5.3 Private life of users

With the exception of the files, folders, emails and, generally, any data that a user indicates as private (examples: the subject of an email is "PRIVATE", a folder is entitled "Private use", etc.), administrators may explore the files of users.

When such a search is deemed necessary due to the occurrence of acts of piracy, they must immediately inform the CISO or their deputy, and, where applicable, the CSSI of their entity.

Personal information may only be accessed in the presence of the user directly concerned, and solely with their written consent. The only exception to this rule is in the case of an obligation handed down by the legal authority. In this case, the network and systems administrator is authorised to access the personal information of a user concerned by this enquiry, without the written consent of this party.

Section 5.4 Management of traceability in the information and communication system

The administrator records and manages the traceability and event logs of the information and communication system. For the entire legal archiving period set out, they duplicate, back-up and preserve traces and event logs provided for by the declaration submitted to the CNIL.

Section 5.5 Management of user information archiving

They may save and archive certain drives, including those that store user information and emails, in order to ensure the business continuity of the information and communication system.

Section 5.6 Management of access to IT or telephone equipment

They may prohibit any information flow (web, email, file transfer, telephone, video, etc.), as well as any IT or telephone equipment that poses as security risk (examples: virus, ransomware, Trojan horse, etc.), or which violates the charter or the ISSP of the École polytechnique.

They may carry out any preventive searches for vulnerabilities on the private or non-private IT or telephone equipment connected to the information and communication system.

Section 5.7 Equipment configuration rights

In the event that IT or telephone equipment is infected with a virus, the administrator may restore this piece of equipment to "factory settings", at the expense of the locally stored data.

The user acknowledges the administrator's right to carry out this task, even if this is to the detriment of the data stored locally on the equipment.

Section 5.8 Duty of the user to back-up their personal information

The user agrees that a potential loss of data stored locally on their computer equipment shall not penalise the École polytechnique or its partners.

To this end, they agree to only save the data they produce in storage areas provided by the École polytechnique and the laboratories: EDRMS, file server, etc.

ARTICLE 6 : GENERAL SECURITY RULES

All users are responsible for their use of the digital resources of the École polytechnique. They must therefore personally contribute to security, so as not to create a weak link for the information and communication of the École polytechnique. In particular:

Section 6.1 Management of digital user names

All users must choose secure passwords, which, *as a minimum requirement*, comply with the recommendations of the ISSP of the École polytechnique. The administrator may test the strength thereof.

These passwords must be kept secret; they must not be written down; they must not be saved on systems external to the École polytechnique (example: synchronisation of passwords through a browser), and under no circumstances must they be communicated to third parties.

They must be changed at the request of the administrators.

Section 6.2 Identity fraud

Each account is personal and corresponds to privileges connected to the user's activity.

A user must not use accounts other than those for which they have received authorisation.

They must refrain from any attempt to use or decipher the password of another user, or risk disciplinary or legal sanctions.

Any session associated with a user account is strictly personal. Users should not leave IT or mobile telephone equipment unattended without logging off from their session.

Section 6.3 Use of tools that have an impact on the security of the information system

The use or development of computer programmes or the implementation of technologies that knowingly jeopardise the security of the information and communication system of the École polytechnique or the national or international networks (examples: viruses, unfinished code, vulnerability scanners, etc.) is forbidden.

In particular, users may not claim a teaching or demonstrative intention in order to be exempt from disciplinary sanctions or potential legal proceedings that the École or the legal authority may have a right to bring.

Section 6.4 Accountability

Users must inform the security managers of the École polytechnique (CISO, Security officer and their deputies) of any violation, attempted violation or suspected violation of the information and communication system as soon as possible.

Section 6.5 Connection of IT equipment

Users must not add IT or telephone equipment without the authorisation of an administrator or the information and communication system security manager.

The temporary connection of a private computer or mobile telephone to the networks accessible on the École polytechnique campus is authorised, subject to the rules related to these networks.

In accordance with section 5.6, administrators reserve the right to block any equipment that fails to adhere to this rule, at any time.

Section 6.6 Observation of security failures

Users agree not to exploit possible security failures, malfunctions or configuration defects.

They must immediately inform solely their administrator thereof, copying in the CISO, and not communicate this information publicly.

The administrator may sometimes choose not to provide a correction if the correction is unavailable or if it is considered to lead to other problems, after having informed the CISO and the ISD.

More generally, users must be vigilant and inform administrators of any anomalies, and follow their instructions.

Section 6.7 Protection against viruses

Users have a duty to protect the equipment they connect to the information and communication system of the École polytechnique, or to ensure that this equipment is protected (examples: anti-virus with up-to-date virus signatures, security updates, etc.).

At the request of the ISD, users must be capable of providing proof of compliance with this obligation.

Section 6.8 Professional information security

Users must ensure the security, confidentiality, integrity and availability of their professional information, including their email. That implies ensuring this information is backed up at a frequency appropriate to professional requirements, and that their storage space is durable.

Except in the case of a specific restriction (incompatible equipment, legislation specific to a country), encryption[3] is mandatory when using mobile computing solutions (laptops, mobile telephones, USB keys, external hard drives, and, generally, any portable storage device).

Section 6.9 External use of the École's digital resources

In the event of travel to a country whose legislation prohibits data encryption, or requires users to provide the local authorities with their passwords or encryption keys, the users must comply with the laws, and not import encrypted material or transport sensitive data.

The use of external services (examples: drive space, email, desktop) and data servers (examples: Web, ftp, RDP) that do not have contractually guaranteed confidentiality, integrity or availability is not recommended. Before using such services, the user must ensure that no data is deemed ineligible for these services due to the sensitivity thereof (e.g.: personal information, trade secrets, etc.).

[3] Action to make data unreadable in reverse, using a password or a digital key

At the time of departure on assignment, particularly abroad, users must take note of the traveller advice set out by the ANSSI (use of dedicated equipment, no sensitive data, no data in violation of local laws).

Section 6.10 Theft of IT or telephone equipment

Users must declare any theft of IT or telephone equipment to their administrator, their line manager and the ISD assistance centre as soon as possible. These departments shall then take the appropriate measures.

A complaint must be lodged by the user, who shall send a copy of the receipt to the ISD.

Section 6.11 Connection to wireless networks

Users must be vigilant when connected to unsecure wireless networks, in particular in public areas. Even when they are not ploys intended to intercept user log-in details, the security of these networks is low. In this context, the use of a VPN-type tool is recommended.

Section 6.12 Regulation of the supervisory authorities

When concerned, users must adhere to the rules set out by their supervisory authorities (examples: CNRS, INRIA, etc.), so long as these are compatible with the rules of the 'École polytechnique.

ARTICLE 7 : RESPECT OF INTELLECTUAL PROPERTY

Section 7.1 Reproduction or de-compilation of software

The reproduction of commercial software other than for the creation of a back-up copy by the legal holder of the rights of use is prohibited.

The de-compilation of proprietary software is prohibited.

Section 7.2 Installation of digital components subject to the copyright, authors' rights or DRM

It is forbidden to install a system, font, or any other file in violation of authors' rights, copyright, DRM and associated licences on the information and communication system of the École polytechnique or any equipment connected to this information system.

The licences of free software must naturally be respected.

Section 7.3 Professional software installed on private equipment

The professional software provided by the École polytechnique on personal IT or telephone equipment must be removed at the time of departure from the École polytechnique or one of its laboratories.

Section 7.4 Archiving of documentary resources

Aside from the back-ups provided for in the context of business continuity, the large-scale and systematic archiving of the documentary resources internal to the École polytechnique and its laboratories (example: websites, files, etc.) using a back-up robot or any other software that offers this functionality is prohibited.

ARTICLE 8 : CONFIDENTIALITY OF INFORMATION

Section 8.1 Rights to access information

All users are responsible for the reading and editing rights they grant to other users for their files and folders.

However, it is forbidden to obtain information held by other users, even if these parties have not correctly protected this information.

As a result, users must not attempt to read, copy, disclose, or modify the files of another user without explicit authorisation.

Sharing of files from a computer is forbidden.

Section 8.2 Hosting of information

Users must make use of the file sharing or documentary management servers of the École polytechnique and its laboratories, as well as those of the Renater operator or a host approved by the CISO or their deputy (examples: CNRS cloud, private operator based in France, etc.). The use of non-managed, remote hosting (examples: failure to protect personal information, absence of a service contract with the École, submission to the "patriot act" for restricted-use data) is not advised (see section 6.9).

Section 8.3 Interception of communications between third parties

Users must not attempt to intercept communications between third parties.

Section 8.4 Adherence to confidentiality obligations with a third party

Uses are required to take the necessary data protection measures to guarantee adherence to the confidentiality obligations undertaken by the École polytechnique with regard to third parties.

Section 8.5 Personal data processing

Any processing of personal data must comply with the processing declaration submitted to the CNIL and the consent obtained at the time of collecting this information. The data protection correspondent (CIL), and, from May 2018 onwards, the data protection officer (DPO), must be informed of any proposed processing of personal data on the information and communication system of the École polytechnique, in order to assist the person in charge of the processing with matters related to compliance with the GDPR regulation.

Section 8.6 Service continuity

In the event of the absence of a user, any measure necessary for the continuity of the service may be implemented, so long as this does not violate the rules described in this charter and in the ISSP of the École polytechnique[4] (examples: transfer of files, temporary or permanent access rights to persons on a "need to know" basis, including the potential authorisations required).

Section 8.7 Data confidentiality

Users must be extremely vigilant with regard to data considered as sensitive under the terms of the information and communication system security policy.

In particular, they should not transport or deposit sensitive data on unreliable devices or services without protection (such as encryption).

Access to sensitive data from unsecure computers or networks is prohibited.

The sharing of data from a computer is prohibited (users must share their data through a file server or a documentary management server authorised by the information and communication system security manager of the École polytechnique, or as an attachment through the email service of the École polytechnique or a laboratory).

When viewing sensitive information, users must be vigilant with regard to the traces left: (examples: browser history, passwords, cache, cookies).

ARTICLE 9 : RELATIONS WITH REMOTE SITES

Section 9.1 Connection to a remote site

It is forbidden to connect or attempt to connect to a remote site without this site having provided due authorisation.

Any VPN or encryption network used for illegitimate or illegal purposes is forbidden.

[4] The email system of the École polytechnique is an exception to this (closure, followed by destruction of the email account after the minimum period set out in section 4.8).

Section 9.2 Correct functioning of the information and communication system

It is forbidden to engage in acts that knowingly endanger the security or operation of the local or remote information systems and telecommunication systems, or harm the reputation of the École (example: redirection of institutional domain names to an unmanaged website) using the digital resources belonging to the École polytechnique or while connected to the computer networks of the École polytechnique.

Section 9.3 Sharing of information with a remote site

Users must be vigilant when entering personal information online, in particular due to the increased incidence of phishing emails.

The École polytechnique cannot be held liable for damage suffered when such information is disclosed.

The administrator reserves the right to block the access of a user that is the victim of phishing, in order to protect the information, communication and audit system, for the entire duration they deem necessary.

From a solely educational perspective, the CISO or their deputy may organise phishing-type attack simulations on all or some of the users. The results of this simulation are confidential, and cannot be used for the purpose of scoring or measuring the performance of a user.

ARTICLE 10 : ELECTRONIC EXCHANGES

Section 10.1 Duty of confidentiality

No party may express themselves in the name of the École polytechnique or commit the École polytechnique in their exchanges without having due authorisation, or without the role they exercise providing for this.

Section 10.2 Rules of behaviour

Each person must demonstrate the utmost correctness with regard to their contacts in electronic exchanges (emails, chats, social networks, etc.).

Section 10.3 User responsibility with regard to the content of exchanges

Given the legal value of an email, everyone must be vigilant with regard to the content thereof, and ensure they are saved (one year minimum).

Section 10.4 Integrity of electronic exchanges

It is reiterated that no guarantee for the correct transfer and delivery deadline can be provided for emails that are sent or transferred outside of the École polytechnique, due to the functioning of the Internet.

Section 10.5 Publications on a website hosted by the École polytechnique

It is reiterated that any publication on a website hosted by the École polytechnique commits this party and its image.

ARTICLE 11 : MODIFICATION OF THE CHARTER

This charter may be consulted on the Internet servers of the École polytechnique, including the site of the ISD. It may be subject to modifications based on the technical and regulatory developments, the uses and the organisation of the École polytechnique. Only the latest French version is valid; foreign language versions are only provided for information purposes.

ARTICLE 12 : APPLICABLE SANCTIONS

Any user that fails to respect the provisions of this charter may have their access rights suspended and may be liable for legal action taken in relation to the breaches observed.

GLOSSARY

[ANSSI]: French National Cybersecurity Agency. This national-scale department works under the Secretary general for defence and national security (SGDSN), the authority in charge of assisting the Prime Minister in the exercise of his responsibilities regarding defence and national security.

[AQSSI]: Autorité Qualifiée de la Sécusité des Systèmes d'Information - Qualified Authority for Information System Security.

[Authors' rights]: Set of rights held by an author or their beneficiaries (heirs, production companies) to original works and the correlative rights of the public regarding the use and re-use of these works under certain conditions.

[CIL]: French data protection correspondent. Refers to the person in charge of managing the implementation of the provisions of the CNIL and GDPR regulations at the École polytechnique

[CISO]: Chief information security officer.

[CNIL]: Commission Nationale Informatique et Liberté - French national data protection authority. Refers to the French independent administrative authority in charge of ensuring that information technologies are used in the service of the community and do not cause harm or damage to human identity, human rights, personal privacy, or individual or public liberties

[CNRS]: French national centre for scientific research.

[Copyright]: In English-speaking countries, copyright, often indicated by the © symbol, is all of the exclusive rights to an original work held by a natural or legal person. It therefore refers to all of the laws in force, in particular, in the countries of the Commonwealth and in the United States. It differs from the authors' rights implemented in civil law countries (such as France or Belgium, for example).

[CSSI]: Correspondant Sécurité des Systèmes d'Information - Information systems correspondent. Refers to a systems and network administrator group.

[DPO]: Data Protection Officer. English name of the French "CIL" in the context of the European GDPR regulation. However, the DPO has extended powers, consistent with the new regulatory framework.

[DRM]: Digital Rights Management, an English term that refers to the management of digital rights, the technical protection of authors' rights and reproduction in the digital domain

[EDRMS]: Electronic Document and Records Management System.

[FTP]: File Transfer Protocol is a communications protocol intended for file sharing on a network. It enables files to be copied from one computer to another computer on the network, or files to be deleted or modified on this computer. This copy mechanism is often used to maintain a website hosted by a third party.

[GDPR]: General Data Protection Regulation. Constitutes the new European reference text with regard to the protection of personal information. It strengthens and unifies data protection for individuals within the European Union.

[INRIA]: French national institute for research in computer science and automation.

[ISD]: Information systems department of the École polytechnique

[ISSP]: Information Systems Security Policy

[LDAP]: Lightweight Directory Access Protocol is a protocol that enables the consultation and modification of directory services.

[RDP]: Remote Desktop Protocol is a protocol which enables a user to connect to a remote Windows computer, in order to access applications and data on this remote computer.

[RENATER]: Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche - National Telecommunications Network for Technology, Education and Research.

[Session]: In data processing and telecommunications, a session is a specific period during which a digital device is communicating and carrying out operations for a client - a user, software or another device

[VPN]: Virtual private network. Refers to an inter-network connection that enables two different local networks to be connected using a tunnel protocol, which is usually encrypted, in order to protect the content of the exchanges from surveillance or fraudulent modification of the data exchanged.