Université Grenoble Alpes

Charter for the use of the EPE information system

(This English version is provided for information purposes only)

Table des matières

Preamble

The Establishment has an information systems security policy (PSSI) consistent with the State's PSSI (Prime Minister's Circular No. 5725/SG of July 17, 2014):

The aim of the policy is to define a precise framework for managing the security of information systems at the sites, in order to enable continuous improvement and guarantee the availability, integrity, confidentiality and traceability of data against the main risks that could affect the system, such as intrusion, data corruption, data disclosure or loss, and misuse of IT resources.

It commits each structure and each user to his or her level of responsibility.

The "Charter for the use of the information system" (IT Charter) specifies the rights and duties of each of the parties involved.

By "**information system**" is meant all the data and hardware, software, applications, databases and telecommunications networks that may be made available to the "user".

Nomad computing such as personal assistants, laptops, mobile phones is also one of the constituent elements of the information system.

By "**user**" is meant any person who is intended to hold a computer account or to have access to the resources of the information system, regardless of his or her status.

This includes in particular:

- any titular or non titular agent contributing to the execution of the missions of the Public Service of Education and Research;

- any student enrolled in the institution;

- any person exterior to the institution, visitor, guest, service provider having contracted with the institution.

By "**professional data**" is meant all the data, files and processing managed by the institution within its activity, whether it be research, teaching, administrative or cultural.

The proper functioning of the information system presupposes compliance with the legislative and regulatory requirements that apply, and in particular, the security, processing performance and conservation of professional data.

The present Charter defines the rules of use and security that the institution and the user agree to respect: it specifies the rights and duties of each.

Considering the commitments of the UGA:

The UGA brings the present Charter to the user's attention.

The institution implements all necessary measures to ensure the security of the information system and the protection of users.

The Establishment facilitates the access of users to the resources of the information system. The resources made available to them are primarily for professional use, but the Establishment is required to respect the residual use of the information system for private purposes.

Considering the user's commitments:

The user is responsible, in any place, for the use he makes of the information system to which he has access. He has an obligation of discretion and confidentiality with regard to the information and documents he produces or to which he has access. This obligation implies compliance with the rules of professional ethics and confidentiality[1].

Users have a particular responsibility in the use they make of the resources made available to them by the institution.

The user is subject to the respect of the obligations resulting from his status or his contract.

[1] In particular, patient confidentiality in health related fields

The following is established:

Article I. SCOPE OF APPLICATION

The rules of use and security included in this Charter apply to the Establishment as well as to all users.

This Charter does not govern usage specifically relating to the activity of trade unions or employee representative organizations.

These rules apply to any person authorized to use the Establishment's IT resources, including shared or outsourced IT resources, and extend to external networks accessible via Establishment networks.

Article II. ACCESS RIGHT TO INFORMATION SYSTEM

The access right to information systems is temporary. It is withdrawn if the user's status no longer justifies it and, unless expressly requested, no later than 3 months after the user is no longer intended to hold a computer account.

It may also be withdrawn, as a precautionary measure, if the user's behavior is no longer compatible with the rules set out in this Charter.

Article III. DATA PROTECTION

The user is responsible for his/her professional data, or those to which he/she has access in the scope of his/her duties. In particular, he/she must ensure that his data is backed up, and be vigilant about the access rights he/she gives other users to this data.

The user must ensure the protection of sensitive information (for which a direct or indirect need for confidentiality has been identified); in particular, he/she must avoid communicating or transporting it without protection (encryption) via unreliable media (messaging, USB keys, laptops, external disks, etc.) and must not place it on an external server or one available to the general public.

Measures for the preservation of professional data are defined with the designated manager within the Establishment.

Article IV. CONDITION OF USE OF IT FACILITIES

Section IV.1 PROFESSIONAL VS. PRIVATE USE

As part of its activity, the information systems are made available to the user.

Use of the IT facilities of the Establishment exclusively covers purposes of research, teaching, documentation, administration or other aspects of university activity. Unless authorised, these systems cannot be used for the operation of projects which are not associated to the Establishment or to projects assigned to the user. They may, however, be used for private communication under the conditions described below.

Residual usage of IT facilities for private purposes must be non-profit activities and moderate, in terms of frequency, volume and duration. Whatever the case, the additional resulting cost must remain negligible in relation to the overall operating cost.

This usage must not have a negative effect on the quality of work provided by the user, on the time the user dedicates to his/her working duties or to the proper functioning of the Establishment.

All information is considered professional, with the exclusion of data explicitly designated by the user as relative to his/her private life, regardless of the medium (computers, USB keys, phones, etc.) or the service used (storage space, messaging, etc.). Thus, it is the responsibility of the user to store data of a private nature in an appropriate area dedicated explicitly[2] for this purpose or to indicate the private nature of the data on the resource[3]. The user is responsible for the protection and backup of private data.

The user is responsible for his private data space. At the time of his/her final departure from the Establishment, it is his or her responsibility to delete his/her private data space. The Establishment does

[2] For example, this space may be named "_private_" or "_prive_"
[3] For example, "_private_name_of_object": the object may be a message, a file or any other digital resource.

not have the duty to maintain this space. In the event of the user's death, his/her private spaces will be deleted.

Private usage of the IT facilities must comply with the applicable laws. In particular, the storage, dissemination ou exporting of images of a paedophile nature, or the dissemination of sexist, homophobic, racist or anti-Semitic material[4] is totally prohibited.

Additionally, in character with the aims of the Establishment, consultation of sites of a pornographic nature within the grounds of the Establishment, outwith a professional context, is forbidden[5].

Section IV.2 MAINTENANCE OF DEPARTMENTAL OPERATION IN CASE OF ABSENCES AND DEPARTURES

In order to ensure continuity of service, the user must give priority to storing his work files in areas shared by members of his department or team. In any case, data not located in a space identified as private is considered as belonging to the institution, which will be able to access it freely.

In case of departure, or prolonged absence, the user informs his hierarchy of the modalities allowing access to the resources specifically made available to him/her. These terms and conditions comply with the security rules set out in Section V.1

Article V. SECURITY PRINCIPLE

Section V.1 APPLICABLE SAFETY RULES

The institution, its supervisory ministry, its access providers and its external academic partners implement appropriate protection mechanisms on the information systems made available to users.

The user is informed that access codes (or any other authentication system) constitute one of the security measures aimed at avoiding malicious or abusive use. However, this security measure does not imply that information tools protected in this way are of a personal nature.

The levels of access granted to the user depend upon the tasks assigned to him/her. The security of the information systems placed at his disposal requires him to:

- Follow the security instructions, in particular, the rules relating to the management of access codes; each user is responsible for the use that is made of them.
- Keep his or her access code(s) strictly confidential and not to reveal it (them) to a third party. In case of doubt about this confidentiality, it is the responsibility of the user to change his/her passwords immediately.
- Respect access management, in particular not to use the access codes of another user, nor to seek to know them ;
- Ensure that he or she never leaves a freely accessible work station unattended.

In addition, the security of the resources made available to the user requires several precautions:

- ✓ On the part of the Establishment:

- Ensure that sensitive resources are accessible only to authorized persons, outside the service continuity organization measures put in place by management.
- Limit the access of the user to only the information for which he or she has been explicitly allowed.

- ✓ On the part of the user:

- Refrain from accessing or attempting to access information system resources for which he/she has not received explicit authorization, even if such access is technically possible.
- Ensure that he/she does not connect devices directly to the local network other than those authorised by the Establishment or those detailed in a user guide defined by the service or the Establishment;
- Not to install, download or use on the Establishment's equipment, software or software

[4] Article 24 and 26 *bis* of *"Loi du 29 juillet 1881"*.
[5] *Code Pénal* (Penal Code), article L 323-1 and subsq. articles

packages without explicit authorization; in case of authorization, downloading and installation can only be done from trustworthy sites.

- Comply with the measures put in place by the Establishment against viruses and various attacks that can harm information systems.
- Not to disturb the proper functioning of computer resources and networks by abnormal manipulation of hardware or software.
- Make all efforts to safeguard the equipment made available to him/her against theft or damage.
- Apply any security recommendations issued by the Establishment.

Section V.2 SIGNALING AND INFORMATION DUTIES

The user must notify, through the Establishment's IT assistance, the person in charge of information system security as soon as possible of any malfunction observed or any anomaly discovered such as an intrusion into the information system, etc. He/she also informs his or her superiors or the hierarchy of any possibility of access to a resource which does not correspond to his/her accreditation.

Section V.3 SAFETY CONTROL MEASURES

The user is informed:

- that to carry out corrective, curative or evolutionary maintenance, the Establishment reserves the possibility of carrying out interventions (if necessary remotely) on the resources placed at its disposal;
- that a remote maintenance is preceded by an information of the user;
- that any information that blocks or presents a technical difficulty in being sent to its recipient can be quarantined, and if necessary deleted (information such as viruses, spyware, spam).
- that the information system may be monitored and controlled for statistical purposes, regulatory or functional traceability, optimization, security or detection of abuse, in compliance with applicable legislation.

Persons in charge of IT facilities monitoring operations are bound by professional secrecy. They must not divulge information that they come to know in the course of their duties if:

- the information is covered by correspondence confidentiality or being identified as such, it falls under the user's private life;
- the information does not jeopardize the proper technical functioning of the applications or their security;
- the information does not fall within the scope of article[6] 40 paragraph 2 of the Code of Criminal Procedure.

Article VI. ELECTRONIC COMMUNICATIONS

Section VI.1 ELECTRONIC MESSAGING

The use of messaging is one of the essential elements for optimizing work and sharing information within the Establishment.

a) *E-mail addresses*

The Establishment undertakes to make available to the user a nominative professional email address for sending and receiving email. The use of this nominative address is then the responsibility of the user.

The nominative email address is merely an extension of the administrative address and does not diminish the professional nature of the messaging system in any way.

A functional or organizational e-mail address can be set up if a service or a group of users uses it.

The management of e-mail addresses corresponding to institutional mailing lists, designating an

[6] The obligation of every civil servant to notify as soon as possible the *Procureur de la République* of any crime or misdemeanour of which he or she becomes aware as a result of their employment.

institutional structure or a group of "users", is the exclusive responsibility of the Establishment: these addresses may not be used without authorization.

b) *E-mail Content*

Any message is considered professional unless it includes a specific and explicit mention indicating its private nature[7] or if it is stored in a private data space.

In order to preserve the proper functioning of the services, limitations may be put in place. In particular, solutions for processing unwanted messages (spam, virus control ...) are deployed.

Messages containing illegal content of any kind are prohibited. This includes content contrary to the provisions of the law on freedom of expression or infringing on the privacy of others (for example: breach of peace by threats, breach of honor by defamation, breach of honor by non-public insult, protection of copyright, trademark protection ...).

Electronic exchanges (letters, discussion forums, etc.) must respect the correction normally expected in any type of exchange, both written and oral.

The transmission of classified data[8] is prohibited unless specifically approved and the transmission of so-called sensitive data must be avoided or carried out in encrypted form.

c) *Sending and receiving emails*

The user must be vigilant with regard to the information received (misinformation, computer virus, attempted fraud, chain letters, etc.).

He must make sure that the distribution of messages is limited to the recipients concerned in order to avoid the mass distribution of messages, unnecessary congestion of the messaging system as well as a degradation of the service.

The user must also ensure that only the tools provided or authorized by the institution are used to manage his/her messaging system. Any recourse to external service providers[9], in particular the general public, for the transmission, reception or storage of messages is prohibited in the professional context.

The user sends his/her messages to groups of people through institutional mailing lists as soon as they exist for the use in question; he/she prefers functional addresses to nominative addresses

d) *Legal status of emails*

According to the law[10], electronic writing has the same evidentiary force as paper writing, so electronic messages exchanged with third parties can legally represent a contract.

The user must therefore be vigilant about the nature of the electronic messages he exchanges in the same way as for traditional mail.

e) *Email storage and archiving*

Each user must organize and implement the means necessary to preserve messages that may be indispensable or simply useful as evidence of a particular activity.

In this respect, they must in particular comply with the rules defined in this Charter.

Section VI.2 INSTANT MESSENGER (CHAT)

Certain departments, particularly in the context of telecommuting, may recommend the use of the Establishment's instant messaging system.

The use that must be made of it ensures that the same principles are respected as for messaging, particularly with regard to the quality and content of the content exchanged.

Section VI.3 INTERNET

We remind you that the Internet is subject to all the rules of law in force. The use of the Internet (by Intranet extension) constitutes one of the essential elements for optimizing work, pooling and accessibility of information within and outside the Establishment.

Internet is a working tool open to professional uses (administrative, educational or research). While

[7] For example, e-mail containing the terms ("private" or "prive") in the subject of the message
[8] This term refers to classified defence data which covers *confidentiel défense*, *secret défense* and *très secret défense* data
[9] With the exception of institutional partner providers and explicitly authorized tools.
[10] Articles 1366-1367 of the Civil Law Code (Ordinance n°2016-131 of 10 February 2016 - art. 4)

residual private use, as defined in section III.1, may be tolerated, it is reminded that connections established through the computer tool made available by the Establishment are presumed to be of a professional nature

a) *Publication on the Establishment's Internet and Intranet sites*

The person responsible for the site or the person, explicitly named, responsible for publication, must approve any publication of information on an Internet or intranet site belonging to the Establishment[11].

The publication of information of a private nature (such as a private site) using the IT facility resources belonging to the Establishment is forbidden, unless specifically authorised as defined in a user guide issued by the department or Establishment.

b) *Security*

The Establishment reserves the right to filter or prohibit access to certain sites, to carry out a prior or a posteriori control of the sites visited and the corresponding access times.

This access is only authorized through the security measures set up by the Establishment. Specific security rules may be specified, if necessary, in a user guide drawn up by the department or Establishment.

The Establishment, its supervising ministry, its access providers or its external technical partners reserve the right to prohibit certain accesses, communication protocols, programs or modules that may affect security.

The user is informed of the risks and limits inherent to the use of the Internet through training actions or awareness campaigns.

Section VI.4 DOWNLOADING POLICY

Any downloading of files, in particular sounds or images, on the Internet must be done in compliance with intellectual property rights (Article IX).

Consulting, and a fortiori downloading from sites whose content is contrary to legislation or morality (sites of a pornographic, pedophile, xenophobic nature...) may be a criminal offence. This activity is strictly prohibited in the Establishment during or outside working hours. It may be subject to penal and/or administrative sanctions.

The Establishment reserves the right to limit the downloading of certain files that may prove to be large or present a risk to the security of information systems (viruses likely to alter the proper functioning of the Establishment's information system, malicious code, spyware ...).

Article VII. TRACEABILITY

The Establishment is legally obliged to set up a system of logging of Internet access, messaging and data exchanged.

The Establishment reserves the right to implement traceability tools on all information systems.

The Establishment has adopted a "general policy for the management of computer logs", which is recorded in the processing register of the Establishment. It mentions in particular the conditions and duration of conservation of traces of connections or use of services, and the methods of expression of the right of access available to users, in application of the modified French Data Protection Act of 6 January 1978 and the European General Data Protection Regulation (EU)2016/679 (GDPR).

Article VIII. COMPLIANCE WITH PERSONAL DATA PROTECTION

The user has the obligation to respect the legal provisions regarding the automated processing of personal data, in accordance with the modified law n° 78-17 of January 6, 1978 called "Informatique et Libertés" and the European General Data Protection Regulation (EU) 2016/679 (GDPR).

Personal data is information likely to identify, directly or indirectly and by any means whatsoever, the natural persons to whom it relates.

All creations of files containing this type of information and related processing requests, including when they result from the extraction, cross-referencing or interconnection of pre-existing files, are subject to

[11] By using the IT resources made available to the user.

legal obligations and must have been the subject of an instruction by the institution's Data Protection Officer (DPO).

In addition, in accordance with the legal provisions, each user has rights relating to data concerning him/her, including data concerning the use of information systems: information, consent, opposition, limitation, access, rectification, portability, omission, notification of data violation, contestation of an automatic decision, right to compensation.

These rights can be exercised with the DPO of the institution.

Article IX. RESPECT FOR INTELLECTUAL PROPERTY

The Establishment reminds you that the use of IT means implies the respect of its intellectual property rights as well as those of its partners and more generally, of all third parties holding such rights.

Consequently, each user must:

- use the software under the conditions of the subscribed licenses;
- not reproduce, copy, distribute, modify or use the software, databases, web pages, texts, images, photographs or other creations protected by copyright or private rights, without having obtained prior authorization from the holders of these rights.

Article X. LIMITATION OF ACCESS

In the event of non-compliance with the rules defined in the present Charter and the terms and conditions defined in the user guides, the "legally responsible person" of the Establishment or the chief information security officer (CISO – *RSSI in French*) may, independently of the legal or disciplinary actions that may be taken against the users, limit access as a precautionary measure.

"legally responsible person" refers to any person with the capacity to represent the Establishment (university president, institute director, etc.).

Any abuse in the use of the resources made available to the user for extra-professional purposes is subject to sanctions. They are decided by the disciplinary section of L'UGA provided for in article L 712-4 of the education code. The penalties incurred are set by Decree No. 92-657 of July 13, 1992, as amended, establishing the disciplinary procedure in Public Scientific, Cultural and Professional Establishments (EPSCP).

Article XI. ENTRY INTO FORCE

This document annuls and replaces all previous documents or charters relating to the use of the Establishment's IT facilities.

It will be effective in each institution on the date of its approval by the competent authority.

It is an Appendix to the Internal Rules and Policies.