1 Preamble

The present IT Charter defines the general conditions of use of the information systems within Institut Curie's Research Center and Head Office. Its objective is to inform users about security requirements. Efficient operation of the information system is based on the observance of legal and regulatory provisions, in particular rules aimed at guaranteeing security, processing performance and protection of data.

1.1 Definitions

- **Establishment** here refers to Institut Curie's Research Center, Head Office, or both.
- **Internal user:** Any natural person working on Institut Curie's sites and, as such, having an identifier in the computer directory of the Establishment.
- **External user:** Any natural person who does not have an identifier in the Establishment's computer directory, accessing the Establishment's Information System or the Internet for the purposes of professional usage linked to Institut Curie's activities.
- The **Information System** is the organized set of technological resources (hardware, software, applications, databases and local telecommunication networks) and organizational and human structure, for the collecting, storage, processing and dissemination of information.
- **Terminal:** Any electronic device, provided by the employer or belonging to Users, used to access the authorized professional or personal Information System: desktop, laptop, or tablet computer, fixed or mobile phone, fax, etc.
- **BYOD:** Bring Your Own Device refers to the use of any personal Terminal for professional purposes.

1.2 Scope of application

This Charter applies to the Establishment as well as to any internal or external User of the Information System.

2 Terms of use of the Information System

The Establishment restates that the tools made available to Users such as telephone, videoconferencing, printer/copy/fax, Internet, message service and collaborative work tools are designed for professional use.

Under certain conditions, Users may connect to the Establishment's network with their own Terminal by wire, corporate Wi-Fi or remote access (VPN-like). They must inform the ISD[1] before any connection attempt. The ISD shall provide users with all the necessary configuration information. The Establishment does not however guarantee compatibility with all Terminals provided by Users.

2.1 Access rights to the Information System

Access rights to the Information System are based on the user account.

A user account is defined by a unique identifier and a password. It grants the User access rights to the Establishment's IT resources, defined according to the position and profile of the User.

A user account, which is linked to one and only one natural person, is strictly personal and confidential, and non-transferable. Users undertake not to communicate, nor transfer their identifiers to third parties.

Users bear sole responsibility for the use of their accounts, as well as for any direct or indirect prejudice caused to themselves or third parties resulting from the use of the computer systems. Users undertake

- To properly protect their password as described in the note included in the Appendix. Users must not use the same password for their professional and private applications.
- To not falsify or intentionally mask their real identity. Any usage of the Information System using a User's account will be considered as having been done by that User, unless proven otherwise.

[1] *ISD: Information Systems Department*

It is strictly forbidden

- To put in place any means of circumventing access controls to the Information System.
- To give access to the Information System to any person who is not duly registered by the HRD[2] or the ISD.

2.2 Residual private use

The residual private use of tools and social networks can be tolerated within the following limitations:

- It is non-lucrative and reasonable, both in frequency and duration.
- It does not hamper the quality of Users' work, the time they devote to it or the proper operation of the service.
- It does not damage the image or reputation of the Establishment (participation in forums, blogs or discussion groups that propagate messages of terrorist, pedophilic, hateful, racist, or abusive nature or that infringe public order or moral principles, etc.)
- It complies with the regulations in force.

2.3 Management of prolonged absences and departures

In case of departure, or prolonged absence, Users inform their supervisors of the means enabling access to the resources that were specifically made available to them. In any case, the data that is not located in a place identified as private[3] is considered the property of the Establishment, which may dispose of them freely.

The departure of a User results in the disabling of their information system account according to the provisions described in the Appendix.

Users are responsible for their private space, and they must recover the contents of this space upon final departure, and free up the space occupied in the Information System. The Establishment may not be held liable for the conservation of data included in this space.

3 Communication tools

3.1 Electronic messaging

Email address

The Establishment provides each User with a personal email address linked to a mailbox enabling them to send and receive electronic messages.

Each User is responsible for the use of their personal address. Thus, the User undertakes:

- To use this email address for strictly professional purposes, except for the cases provided for in Article 2.2 of the present Charter.
- To remain vigilant about messages received, in particular unsolicited email ("spam") that may contain false or fraudulent information, viruses, or links to malicious sites. Messages and attachments are indeed often the main vectors of cyberattacks.
- Not to use for professional purposes email boxes other than those provided by the Establishment or Supervising authorities (INSERM, CNRS, etc.), and even more so "free" email addresses (such as Gmail,

[2] *HRD: Human Resources Department*

[3] *For example, a folder or file including in its name "private_surname_name", or named "perso" or "personal"*

Live or Yahoo) that use the data exchanged. The use of third-party messaging applications is forbidden in particular to exchange sensitive data[4].

- In all cases, to behave in a way that could be expected in any type of exchange with correspondents.

Electronic messages

Any message received or sent using the professional address is considered to be of a professional nature, except when explicitly mentioned as being of private character[5], or if stored in a private data space.

If this is not indicated, and when necessary for the pursuit of the Establishment's activities, the employer may freely access messages at any moment.

However, Users must not turn all of their professional messages into private correspondence. In cases of risks to security, service continuity, or of being held liable, the Establishment may access the files or content of an electronic mailbox identified as "private" in the presence of its User, or in their absence if they have been duly informed.

Messages content

It is strictly forbidden to exchange messages that include:

- Illicit content of whatever kind. In particular, it is forbidden to distribute contents that are harmful to the privacy of others (harmful to tranquility through threats; harmful to a person's honor through defamation or insult).
- Harmful to the image and reputation of Institut Curie and/or its Establishments.
- Harmful to the integrity of the Information System of Institut Curie and/or its Establishments.

3.1.1 Legal status and value of messages

It is recalled that Institut Curie is liable for electronic messages. Users must therefore remain vigilant concerning the nature of messages exchanged.

3.1.2 Control and analysis of the messaging system

In order to maintain the proper functioning of the network and services, control mechanisms for the messaging system have been put in place; limitations may be applied concerning the size of messages sent and received, the number of messages sent per time period, or the overall capacity of email boxes.

3.2 Internet

Internet is a working tool to be used for professional purposes, even if a residual usage for private purposes may be tolerated, as mentioned earlier.

When Users use the Internet, they leave connection traces on external servers, in particular concerning the Establishment. Users therefore undertake to remain vigilant when they use the Internet in order not to cause prejudice to Institut Curie and/or its Establishments.

Control and analysis of the Internet
Internet access is authorized only through the security procedures implemented by the Establishment, which ensure:

[4] *According to the CNIL (French National Commission for Data Protection and Liberties), these are personal data that give a direct or indirect indication of racial or ethnic origin, political, philosophical, trade union or religious opinion, sexual orientation, offences, criminal convictions or security measures, social security number, assessment of social difficulties of persons, biometric data, genetic data, or healthrelated data.*
[5] *For example, messages that include the word "privé" (private) in their object or subject.*

- The filtering of web sites: Illegal sites (with content promoting terrorism, sale of weapons or illegal drugs, etc.) or sites with no relation to professional activities (pornography, online gaming).
- Traceability of Internet access: Connection data is recorded in trace files and kept for a period of at least six months, in conformity with the declaration made to the CNIL. Administrators may analyze traces as part of maintenance work or the search for technical malfunction, while respecting the right to privacy and confidentiality.

3.3 Phone services

The Establishment reasserts that the use of phone services is intended for professional purposes and that only residual use for private purposes will be tolerated.

Listings may be established, and in case of manifestly excessive use of phone services for private purposes, the User will be informed and sanctions may be taken if necessary in conformity with applicable legal rules.

3.4 Social networks

Social networks offer a wealth of information for experts in data collection and hackers.

It is forbidden to communicate on a social network about and on behalf of the Establishment, in the private or professional sphere, except with the express authorization of the employer.

Publications on social networks are subject to the same rules as emails, blogs, personal pages or any other means made available to the User by the Establishment.

3.5 Online services

In order to guarantee the continuity of services, Users must opt for the storage of their professional files on the Establishment's servers, which provide secured working spaces shared by the members of their teams.

Externalized storage and sharing of files on the cloud offer a practical means to access data in all circumstances. Their use in a professional context must however be subject to precautions in terms of security and confidentiality, as specified in the Appendix. In particular, their use is prohibited concerning health data and information of a personal nature.

3.6 Remote access

Remote access enables Users to access the Establishment's Information System remotely in a secure manner.

Depending on the level of sensitivity of data which Users want to access, several authentication procedures may be required: user account including an identifier and a password and/or an additional code requiring validation.

The remote access service is subject to the same terms of use of the Information System as those applied within the Establishment, in particular those concerning the confidentiality and non-transferability of user account and its corresponding access rights.

4 Data protection

The use of personal terminals for professional purposes (BYOD), in particular for email access and access to documents stored on the Establishment's servers, is increasingly widespread. However, such terminals introduce a high risk of professional or private data loss or theft, and are seldom protected using encryption[6].

Thus, to limit the risks of loss of data, Terminals and storage devices (USB keys, external hard drives, etc.), both professional and personal, must be encrypted if they contain professional data.

[6] *Encryption: method that reinforces the security of a message or file by blurring its content, so that it can only be read by people who have the appropriate encryption key*

[7] *Information System Security Officer*

It should however be noted that encryption is a protection only against data disclosure, and not against data loss. It is therefore necessary to create copies of data by executing regular backups on the Establishment's servers.

5 Duty to report

Usesr have a duty to report to their supervisors, or to the ISSO[7] or, failing that, to the ISD, as soon as possible:

- The loss or theft of their password, or identity theft
- The loss or theft of devices containing professional data, whether these devices be personal or provided by the employer
- Any malfunction or abnormality detected, such as a virus or an intrusion into the Information System.

Generally speaking, any suspicion of risks to the security of the Information System or any substantial breach of this Charter must be reported.

The Establishment may take all necessary measures to protect its interests and the confidentiality of data contained in the lost or stolen devices, in particular by deciding to delete all data, as far as possible.

6 Intellectual Property

The use of IT resources implies observance of intellectual property rights of Institut Curie and its partners, and more generally any third party owning such rights.

Thus, Users undertake:

- To use software under the conditions of the licenses subscribed.
- Not to replicate, copy, distribute, modify or use files (texts, sounds, images, software or other creations protected by copyright) without prior authorization from the owners of those rights.

The Establishment reserves the right to block any manifestly unjustified downloading of files containing data subject to copyright.

7 Compliance with the Data Protection Act

Users have an obligation to comply with the legal terms on the automated processing of personal data defined in the French law entitled *Informatique et Libertés* ("Data Protection Act").

Personal data refers to any information that make it possible to identify, directly or indirectly, a natural person by an identification number or one or several of their characteristics.

Any User who, in performing their work, is called upon to create files subject to the terms of the Data Protection Act, in other terms containing personal data, is responsible for the observance of the terms required by the CNIL in compliance with the internal procedures of the Establishment. They must ensure that data processing is set up and maintained in compliance with the legal provisions, and to inform the ISSO or, failing that, the ISD.

It is recalled that it is illegal to transfer a file containing personal data not declared to the CNIL to a third party.

8 Control and analysis

The Establishment is legally obliged to set up a logging system[7] of access to the Internet, email, phone services, and all applications and data exchanged through the Information System.

Tracking mechanisms are set up according to the statements filed with the CNIL[8].

---

[7] *Logging of technical connection data such as access times, IP address of the User's Terminal and the server accessed, and specific information such as the address of a Web site ("URL") or recipient of an email.*

[8] *CNIL: Commission Nationale de l'Informatique et des Libertés (French National Commission for Data Protection and Liberties)*

It is recalled that administrators who have extended access are, in addition, subject to increased confidentiality obligations.

In the framework of a legal procedure, these files will be made available to the legal system "for purposes of research, ascertainment, and prosecution of criminal offences".

According to the Data Protection Act, Users have a right to access and correct data concerning them. Access rights to the Information System imply acceptance by all Users of the logging procedures.

9 Applicable sanctions

The Establishment reserves the right to take sanctions against any User who does not respect the terms of the present Charter, in particular in the following cases:

- A User making usage of the IT services in a way that could harm Institut Curie or third parties.
- A User performing acts of computer piracy, for example by distributing or duplicating data subject to intellectual property.
- A User misusing IT resources for extra-professional purposes.
- A User not observing the laws or regulations in force.

Sanctions may range from a warning—with or without a partial or complete, temporary or definitive removal of access rights to the Information System—to contract termination. Civil or penal legal proceedings may arise if necessary.

10 Entry into force of the Charter

The present Charter enters into force as of 2017 August 1st. It supersedes any other document or charter related to the use of the Establishment's Information System.

It is included as an appendix to the internal rules.

Date:

Signature of the person having access to the computer system of the Research Section of the Institut Curie.