RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inserm
La science pour la santé
From science to health

Terms of Use for Access to INSERM's Computing Resources

This document defines the minimal set of norms for using information systems and networks at INSERM. It applies to every user of any Information System from INSERM.

This IT charter aims to provide access to all those information systems in optimal and explicit conditions.

It is available for all interested parties on the intranet site https://pro.inserm.fr. This English version is provided as a translation of the original document. The French version is considered authentic; for any difference in terms, only the French version applies.

Access to any information system requires accepting these terms of use. Failing to abide by these may cause the user's access to be terminated.

For any clarification, users are advised to ask, depending on the topic, the IT correspondent at their Regional Administration, the Data Protection Officer at INSERM, or the Chief Information Security Officer at INSERM.

1 - Definitions

The term "Entity" refers to the structures created by INSERM to accomplish its missions, such as Research Units, Teams, Departments, and/or Administrative Services.

The term "IT resources" refers to the IT means of computation or system management under the responsibility of INSERM, whether local or accessed remotely and the network services under the responsibility of INSERM allowing local or remote communication.

The term "Internet Services" refers to the services offered by third-party organizations and companies, whether or not they are linked by contract with INSERM.

The term "User" refers to people accessing or using an INSERM entity's IT resources and Internet services. The term covers, without limitation, INSERM agents, associated staff, interns, students, or external service providers.

The term "Administrator" refers to people carrying out the functions of management, supervision, or maintenance of IT resources or access to Internet services.

The term "Hardware" refers to computer equipment used by Users (stations, laptops, tablets, mobiles, hardware authentication devices).

2 – Terms of use of IT Resources

The use of *IT Resources* and *Internet Services* is only authorized within the *Users'* professional activity framework.

For an INSERM agent, professional activity is assessed in particular concerning the provisions

of the French “Code de la Recherche” or the Decree 83-975 relating to the organization and functioning of INSERM.

The use of the *Entity*'s *IT Resources* and the connection of any equipment to the network falling within the scope of the *IT Resources* are also subject to authorization.

These authorizations are, unless specifically organized by the *Entity*, issued under the authority of the director of the *Entity*, are strictly personal and nominative and cannot under any circumstances be transferred, even temporarily, to a third party, and are communicated by the *Entity* to the *Administrators* for further action.

These authorizations may be suspended or withdrawn by the authority having issued them at any time.

The *Entity* may also apply specific access restrictions to its internal organization.

3 - Hardware

For the needs of its professional activity, *Hardware* (stations, laptops, tablets, mobiles, authentication devices, etc.) may be provided by INSERM to the *User*. These pieces of *Hardware*, now called *Professional Hardware*, are intended exclusively for professional activity. The *User* must not install software for personal use on this *Professional Hardware*, even if it is technically possible. Any software installation or update requires contacting the *Administrator*.

The *Administrator* may monitor or maintain this *Professional Hardware*, particularly for security reasons. The *User* will be informed in advance of this intervention. The *Administrator*'s personnel in charge of these operations, in particular maintenance or control, are subject to an obligation of confidentiality. They may under no circumstances communicate to a third party the data accessed on the *Professional Hardware* as part of these control and maintenance operations.

However, it is reminded that in the application of article 40 of the Code de Procédure Criminelle, any agent who, in the exercise of his duties, acquires knowledge of a crime or an offense is required to give notice without delay to the public prosecutor and to transmit to this magistrate all the information, minutes and acts relating thereto.

When necessary, the *User* must ensure data protection on this *Hardware* by ensuring their security or backup. If the *Professional Hardware* does not appear to be compliant, he must inform the *Administrator*.

When *Hardware* contains sensitive data, it must be secured by an encryption device. The *Administrator* is responsible for installing these encryption devices on the *Professional Hardware*.

The use of *IT Resources* must be done via this *Professional Hardware*.

The use of Personal *Hardware* is prohibited unless it is impossible to use *Professional Hardware* and subject to prior authorization from the director of the *Entity* and verification by the *Administrator* of the conformity of the Personal *Hardware* with the rules and standards in force at INSERM.

Professional Hardware must be returned at the end of the activity for which it was provided.

4 - Access Control

Access to non-public *IT Resources* by a *User* is subject to access control via appropriate means: passwords, digital certificates, hardware devices, etc. These means of access are strictly personal and nominative and cannot under any circumstances be disclosed or transferred, even temporarily, to another person, colleague, third party, or family member.

Each *User* is responsible for these means of access and must ensure their confidentiality. Physical means must be protected against theft, logical means must be stored securely, and passwords must not be written down or saved on unsecured media.

In the event of loss or disclosure, the *User* must immediately inform the *Administrators* for action (if applicable, to invalidate or replace the means of access concerned if the *User* has not done so on his own cognizance).

The *User* is not authorized to communicate his password allowing him to access the *Professional Hardware* or *IT Resources*. However, when the *User* must, exceptionally, for service needs and temporarily, communicate a password, he must ensure that the person to whom he communicates it is duly authorized by the director of the *Entity*. The *User* must then and as quickly as possible change their password once the need has expired.

The means of authentication used for INSERM *IT resources* must not be reused for another setting. *Users* must ensure not to reuse their passwords or INSERM professional digital certificates in any other context on *Internet services*.

When using an INSERM password or digital certificate recovery mechanism, the *User* must ensure that it is secure, particularly if using a personal *Internet service* such as an external email.

5 – Detailed Terms of Use

The use of *IT resources* must be rational and fair to avoid their saturation or misappropriation.

Notably, a *User*:

- Must apply any security recommendations in force within the *Entity* to which they belong;
- Must follow any rules in force within the *Entity* for any software installation;
- Must apply the rules in force for all of INSERM, including the PSSI (Information Systems Security Policy);
- Must report to the *Administrator* any attempted violation of his account and generally any anomaly they may observe;
- Must not provide unauthorized users with access to *IT resources* through the *Hardware* they use;
- Must not use or attempt to use accounts other than their own or mask their true identity;
- Must not misuse or abuse the rights assigned to them, including reading, modifying, copying, or destroying data when these actions are not legitimate;
- Must lock their workstation when they leave their workstation, including for a short time, to avoid any misuse of *IT resources* or accessible *Internet services*.

The use of *IT resources* must be lawful.

Notably:

- It is strictly prohibited to make copies of commercial software for any use except for a backup copy under the conditions provided for by the intellectual property code. These can only be carried out by the *Administrator*;
- It is prohibited to circumvent the restrictions on the use of software;
- The installation on a computer system implemented by INSERM of software for which the

right of use is acquired privately by a *User* is not authorized;

- The *User* must comply with the terms of the software licenses used at INSERM which are communicated to them;
- The *User* undertakes not to voluntarily cause disruptions to the proper functioning of computer systems and networks (internal or external to INSERM), whether by abnormal manipulation of resources or by the introduction of malicious software known by the generic name of viruses, Trojan horses, logic bombs or the like;
- The *User* undertakes not to constitute files or create processing of personal data, as defined by the General Data Protection Regulations, without obtaining prior written authorization from the director of the *Entity*. All processing and files must be included in the processing register of the legal controller.

These conditions apply without prejudice to the applicable legal and regulatory provisions in force and, in particular:

- The Intellectual Property Code;
- The General Civil Service Code, including the articles relating to the general obligations applicable to public officials (Articles L121-1 to L121-11);
- The Penal Code, including articles 323-1 and following relating to attacks on automated data processing systems (Articles 323-1 to 323-8);
- The law No. 78-17 of January 6, 1978, relating to data processing, files, and freedoms;
- The regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95 /46/EC (referred to as “General Data Protection Regulation” or “GDPR”).

6 – Use of Internet services

The *User* must only use the *Internet services* to which he accesses using INSERM *IT resources* or *Professional Hardware* for the exclusive needs of his professional activities and only in compliance with general principles and rules specific to the various sites that offer them and in compliance with the legislation in force.

7 - Usage of messaging and collaborative work services by Users

Access to INSERM messaging and other collaborative work tools may be available to the *User*.

This access is granted for the sole needs of professional activity.

Residual privacy associated with messaging is tolerated, but any message or document for personal use must be clearly identified as such by the words “private” and their number limited.

Each *User* will work with the *Administrator* to organize and implement the necessary means for preserving messages considered essential or simply useful as evidence. The same will apply if these are kept outside the mail servers (so that these archives are backed up).

Messaging *Users* must take care not to misuse the service, particularly by sending mass messages.

Regarding large attachments, the user must favor data transfer via suitable *IT resources* or authorized *Internet Services* rather than via messaging.

When the documents or messages are particularly sensitive, the *User* will contact the *Administrator* to ensure that these documents or messages are encrypted beforehand.

Using messaging or a collaborative work service for classified data (Restricted Diffusion) is only possible in conjunction with an encryption mechanism approved by ANSSI. Using messaging or collaborative work services for higher classified data is not authorized. The *User* will contact the *Administrator* if they are required to process classified data to ensure that this use complies

with the standards and recommendations in force.

It is not authorized to transfer messages and content to messaging or collaborative work services dependent on external organizations or companies, except supervisory authorities or research establishments to which the *User* or their *Entity* depends. Particular attention must be paid to automated transfers (synchronization, email redirection). The *User* will contact the *Administrator* to deal with this point.

The use of general public tools for messaging or collaborative work is subject to explicit and written exemption from the director of the *Entity* to which the *User* reports and prior authorization from the *Administrator*.

These exemptions are only necessary for documents and messages under the *User*'s responsibility. Collaborative work and exchanges with third parties outside INSERM can be done under the responsibility of this third party with the tools or messaging of said third party.

8 – File Creation

Files owned and/or created by a *User* are presumed to be of a professional nature.

By way of derogation from use for professional purposes, any use of the *IT Resources* for personal purposes must be residual, both in frequency and duration, per the conditions and limits defined below.

As such, *Users* must classify files relating to their private life in a folder bearing the title "personal" or "private", which must in no way be stored on a community location (Intranet, collaborative space, file server, etc.).

In any event, the use of *IT Resources* and *Professional Hardware* for personal storage is limited to reasonable use; it must not, in any way, disrupt the proper functioning of the service and *IT Resources*.

9 - Monitoring – Filtering

To meet the legal obligations incumbent on INSERM, relating to its capacity to:

- provide proof, where applicable, of the proper professional use of the *IT Resources* made available to the *User*;
- to prevent any illicit use of these information systems.

It is carried out in compliance with the information of the persons concerned and the Data Protection Act of January 6, 1978, as amended, and European Regulation 2016/679 of April 27, 2016:

- the deployment of traceability tools (connection logs) for all information systems;
- the deployment of filtering tools (content filtering, URL filtering, protocol filtering, etc.), making it possible to analyze the conditions of use of these means, to prohibit this or that protocol, or even to restrict or prohibit the access to Internet or certain categories of *Internet services*.
- In compliance with the principles of transparency and proportionality, the *User* is notified that the IT security devices (firewalls, access control systems, etc.) put in place by INSERM record traces and that filtering systems are put in place, in particular:
    - for incoming and outgoing messages with antiviral control;
    - for messages whose size or recipient list is too large;
    - for messages from or to a user or an electronic mail server of a clearly hostile nature (massive sending of messages, harassment of a user, etc.);
    - to block messages or access to unauthorized sites based on a list of "keywords";

- more generally, any filtering necessary to preserve the information system's security can be implemented.

The operation of these filtering systems falls within the competence of the *Administrators*.

Any misappropriation, alteration, or modification of these tools or the data collected using these tools is strictly prohibited.

10 – IT Resources Controls

INSERM has the right to control the use of computer resources by *Users* within the limits provided for by law and case law and after prior information of *Users*.

Authorized persons from the Information Systems Department, duly mandated to carry out these procedures, will keep confidential any information they may become aware of on this occasion.

As such, *Users* are informed that the authorized persons of the Information Systems Department who must ensure the normal operation and security of computer networks and systems are required, by their functions, to have access to all information relating to *Users* (messages, internet connection, etc.), including those recorded on the hard drive of their *Professional Hardware*, except for multi-encrypted documents for reasons of confidentiality.

However, the latter are bound by a reinforced obligation of discretion and can only use their administrator rights for strictly professional purposes.

Systematic checks or by sampling or based on elements indicating non-standard use can be carried out on all the *IT Resources* made available to the use, at any time and to carry out any act of protection of the Systems, in particular, to protect against non-compliant use which could be detrimental to INSERM.

INSERM reserves the right, within the framework of these missions, to:

- check incoming and outgoing computer traffic (duration of connection, sites visited, times of visits, items downloaded, etc.), as well as traffic passing through the internal network;
- check certain types of content which are often the cause of incidents (disk space problems, network congestion, chain broadcasting, "cookies", etc.);
- carry out audits to verify that the usage instructions and security and safety rules are applied to the information system resources;
- check the legal origin of installed software;
- filter email addresses or URLs of unauthorized sites;
- to read copies of all professional emails upon request from general management, human resources management, legal and compliance authorities, etc.;
- keep log files of global connection traces for a period not exceeding six months;
- control the use of messaging in terms of volume/number of messages exchanged, size of messages, format of attachments, quantity of disk space used, analysis of messages (selection of words of a pornographic, racist nature, etc.);
- transmit all or part of the available recordings upon request to the judicial authorities.

In the event of a body of evidence suggesting that a *User* is jeopardizing the interests or security of INSERM by not respecting the rules established by this charter, the Information Systems Department reserves the right to provide to the Human Resources Department, upon its written and reasoned request, individual traces of the incriminated connections over a period not exceeding six months.

In addition, in the event of an incident, INSERM reserves the right to:

- monitor the content of information passing through its information systems;
- check the contents of the hard drives of the *Professional Hardware* resources allocated to *Users*;

- make all useful copies for asserting INSERM's rights.

The Information Systems Department monitors IT services over connection times and the most visited sites as part of the mission to protect *IT Resources*. In the event of a disruption caused by the untimely appearance of alerts following attempts to infect systems using computer malware, the Information Systems Department is authorized to carry out any investigations that it deems useful to eradicate said malware.

In the event of non-compliance with this charter by a *User*, the Information Systems Department will be obliged to notify the *User*'s supervisor so that they can decide what action to take.

Depending on the seriousness of the facts, the access rights of the *User* concerned may be suspended.

Any illicitly installed software or suspicious files will be deleted by the Information Systems Department as soon as they are noticed on the *Professional Hardware*.

11 – Processing of Personal Data

As a data controller, INSERM, implements the processing of personal data for to manage its information systems for all *Users*. The legal basis for this processing is legitimate interest.

The purpose of these treatments is, in particular, to ensure:

- management and control of the use of *IT resources*;
- monitoring and maintenance of *IT resources*;
- defining access authorizations to applications and networks;
- the implementation of systems intended to ensure the security and proper functioning of the information systems;
- security of *IT resources* and information systems;
- management of professional electronic messaging and other professional communication systems.

Personal data concerning *Users* may also be processed as part of managing files in which *Users* intervene. In addition, connection logs to *IT Resources* may be collected with *Users*' identities for security reasons.

The data collected is essential for this processing and is intended for the relevant INSERM services and, where applicable, its subcontractors or service providers.

The data collected may be kept for the duration of the contractual relationship plus the duration of legal requirements.

Shorter durations can sometimes be applied depending on the purpose of the processing, such as for connection logs to *IT Resources*, which are kept for six months.

In application of the RGPD legislation, the *User* has a right of access, rectification or erasure, limitation of the processing of his data, a right of opposition to the processing, a right to the portability of one's data as well as the right to define directives relating to the fate of one's data after one's death, which is exercised by email to the address dpo@inserm.fr or by written mail to the attention of the Data Protection Officer, at the following address: 101 rue de Tolbiac, 75013 Paris.

The *User* finally has the right to lodge a complaint with the CNIL.

12 - Applicability

This charter applies to all INSERM agents of all statuses on the one hand, and on the other hand, to all external people, permanent or temporary, using INSERM *IT Resources*.

It will also be signed by all people welcomed at INSERM and having access to said *IT Resources*. This English version is provided as a translation of the original document. Signing this version is considered as approving the original version in French.

LASTNAME / FIRSTNAME:

DEPARTEMENT :

DATE :

SIGNATURE
(Preceded by the words “Read and approved, good for agreement”)

In Paris, the #date#

The Chief Executive Officer
Didier Samuel

For the CEO, and by delegation

#signature1#