Instituts thématiques Inserm

Institut national de la santé et de la recherche médicale

Terms of Use for access of INSERM's computing resources and Internet services

This document is provided as a translation of the original document, which is written in French. In case of a discrepancy between the original text and this document, the original French document will be presumed to be correct.

This document establishes a guide for good practice. Its purpose is to remind of the user's liabilities according to current legislation, and to provide a proper framework of the use of computing resources and Internet services while respecting all relevant legal and regulatory statutes along with a minimum of politeness and respect of other users.

For clarification, please refer to your manager in your Team, Unit, Department, to the RRI[1] at your local Regional Administrative Office, or as a last resort, to the CISO[2] of INSERM.

1 Terms and definitions

We shall designate as "entity" any structure established by INSERM to fulfil its objectives, such as Research Units, Teams, Administrative Services or Department.

We shall designate as "computing resources" any local or remote computer system belonging to INSERM, and any third party system hosted on a network managed by an INSERM entity.

We shall designate as "Internet services" the access to services available over the Internet from non INSERM entities.

We shall designate as "users" persons accessing or using computing resources or Internet services provided by an INSERM entity.

2 Access to computing resources and Internet services

The use of computing resources and Internet services shall be exclusively devoted to professional activities of the users, in due respect of the current legal framework.

---

[1] « Responsable Régional Informatique » ; Regional Computer Manager

[2] Chief Information Security Officer

Professional activity shall be defined as any of those covered by the GIP RENATER[3] charter: research activity, teaching, technical developments, technology transfer, scientific, cultural or technological information dissemination, innovative services experiments, and any administrative and management activity related to the above.

The use of computing resources shared within an entity and the hook-up of any device on the local network require authorization. These authorizations are delivered by the entity Director, are nominative, non transferable, and can be revoked at any time. Any authorization automatically ends when the activity that required it stops, even if that is a temporary suspension.

An entity can also impose additional access restrictions to some or all of its resources and services.

3 Use and Security Rules

Each user is responsible of the proper use of computing and network resources that he or she access to. He or she must also take care of the security of those resources.

Use of computer resources must be rational and reasonable, in order to avoid saturation. Use for personal purposes is strictly forbidden.

Notably, the user

- must follow the security regulations of the entity to which he or she belongs;
- must ensure safe care of his or her data, using the services and products provided by the entity to which he or she belongs;
- is held responsible of any access granted to other users;
- has to notify any unauthorized access to his or her account, and any anomaly he or she notices;
- must follow the relevant rules in his or her entity for the installation of any new software;
- must choose secure passwords, keep them secret, and cannot communicate any of his or her passwords to a third party, even within the same entity;
- must not provide to unauthorized users an access to computing resources or networks by proxy;
- must not access or attempt to access any account that does not belong to him or her, or to hide his or her identity;
- must not attempt to read, modify, duplicate or destroy data that does not belong exclusively to him or her;
- must not leave his or her private or public workspace unattended, thus leaving computing resources or services accessible, unless specifically invited to do so by his or her network or system administrator.

[3] « Groupe d'Intérêt Public »

4 Confidentiality

Access to information and documents on a computing system must be restricted to those belonging to the user and those that are public or shared.

It is strictly forbidden to access restricted information belonging to another user, even if that information is not explicitly protected. This rule applies to all documents, notably private electronic exchanges the user is not party to.

If the user, during his or her missions, has to create files that fall under the statutes of the "Loi informatique et Libertés", the user must have notified or received authorization from the CNIL[4] prior to this, and in consultation with his or her director, the Regulatory Office of INSERM and the Legal Department of INSERM. The user is reminded that these authorizations apply only for the stated purpose, and not for the existence of the file.

5 Software licenses

It is strictly forbidden to make a copy of licensed software for any purpose whatsoever, excepted for the backup copy allowed by the law. Any such backup must be exclusively performed by a designated person.

The user must not install any software for entertainment purposes, and is not allowed to bypass any restriction on the use of software.

Most software provided to users by INSERM is subject to licensing by INSERM. Users are responsible for violations of those licenses; failure to comply is considered malpractice.

Installation of privately licensed software on an INSERM computing resource is strictly forbidden, even if its use is restricted to the licensee.

6 Integrity

The user must not wilfully cause perturbation in the normal operation of computing resources and networks, INSERM or non-INSERM, through the abnormal use of systems, or execution of malicious software.

Any research work that might violate the above rule can only occur with the written sanction of the entity director, and within the framework defined in that directive.

The user must ensure that his workstation and additional dedicated computer resources uses an appropriate protection software to prevent the unintended execution of any malicious software.

[4] Commission Nationale Informatique et Libertés

7 Use of Internet services

7.1 General good use rules

The user must access Internet services for the exclusive purpose of conducting his or her professional activities, and in due respect of any general and specific term of services that apply to those services.

Notably, the user

- must not access or attempt to access a service outside of the terms specified by that service or without the required authorizations from appropriate authorities;
- must not engage in activities that will wilfully put in danger the security or continued operation of the services he or she accesses;
- must not make use of the identity of any other user;
- must not attempt to intercept or eavesdrop on communications between third parties;
- must not use a service to provide confidential information to outside parties;
- must not use a service to store information and documents unless this use is authorized by management;
- must show respect to his or her correspondents in electronic mail or other communication channels;
- must show restraint and not advocate personal ideas that could reflect inappropriately on INSERM or its collaborators;
- must respect the appropriate legislation governing the public expression and publication that could be interpreted as abusive, injurious, racist, slanderous or include pornographic or offensive material.

7.2 Internet publication

Providing to the general public an Internet service that falls under the umbrella of the inserm.fr domain, displays the INSERM logo, or implies its affiliation to INSERM requires the authorization of the DISC[5]. Publication of documents on such a service will fall under the responsibility of the entity's director, with a further check by the DISC, and respect the Terms of Use of Internet in INSERM laboratories.

7.3 Liability

The publication of information and documents to the public engages the personal liability of their author, exclusive of the general liability of INSERM.

8 Monitoring

For technical purpose, and to provide proper technical management of the computing resources and access to Internet services, any use of software and hardware computing resources and any access to networks can potentially monitored, in accordance to the current legal framework including the "Loi Informatique et Libertés".

9 Legal reminders

Any person residing on French territory must respect the French legislation, notably regarding computer security:

[5] Département de l'Information Scientifique et de la Communication

- Loi Informatique et Libertés, January 6th 1978;
- Computer Fraud act;
- Intellectual Property legal framework;
- Loi relative à l'emploi de la langue française, August 4th 1994;
- Cryptology in Communications act.

10 Applicability

The present terms of use applies to all collaborators of INSERM, regardless of position, and to all and any persons working full time, part-time or for a limited duration within the entity, or accessing the entity's computing resources from outside the entity or accessing Internet services through the networks managed by the entity.

It must be included, for informational purposes, into any work contract for non permanent staff that have access to computing resources.

It has to be signed by any third party that is contracted to or has temporary residence in an INSERM entity and has access to INSERM computing resources and networks.

LAST NAME FIRST NAME DEPARTEMENT

DATE

SIGNATURE