# Terms of use of information and communication technologies at the University of Burgundy

---

**Adopted by the Board of the University of Burgundy on June 28, 2007. This Charter constitutes the internal regulations regarding the use of ICT.**

## Preamble

The *information system* consists of all material resources, software, applications, databases and telecommunications networks, which may be made available to the *user*.

Mobile computing, including PDAs, laptops, mobile phones, etc., is also one of the components of the information system.

The proper functioning of the information system requires compliance with legislative and regulatory requirements covering security, the handling of data processing and the conservation of personal data.

This Charter defines the rules of use and security to which the institution and the user agree: it specifies the rights and duties of each.

The Charter is accompanied by a **legal annex** that groups the existing legislation for its implementation. It may be supplemented by a **user's manual** setting out the principal common practices.

The University of Burgundy shall inform the user of this Charter.

## Commitments of the institution

The University of Burgundy agrees to implement the necessary means to ensure the security of the information system and the protection of its users.
It facilitates user access to the resources the information system which are dedicated to teaching, research, documentation and the management of the University.
Resources are made available primarily for academic use, but the institution shall respect the privacy of individuals.

Commitments of the user

The user is responsible, at all times, for any use made of the information system to which he has access. He has a duty of discretion and confidentiality with regard to the information and documents that are accessed. This obligation implies compliance with codes of ethics and professional conduct.

Users have a particular responsibility in their use of resources made available by the University.
In any event, the user is subject to the obligations arising from his status or his contract.

## Article I. Scope

A user is an individual (student, teacher, researcher, engineer, technician, administrative or service personnel, temporary employee, intern, etc.) authorized to access any resource in the information system.

The rules of use and safety instructions in this Charter apply to the institution as well as to all users.

Users who serve as directors of information systems are subject to an additional charter setting forth the details of their specific obligations.

## Article II. Conditions for use of information

### *Section II.1 Private university use*

University information systems are made available to users.

All use for private purposes must be non-profit and reasonable, both in frequency and in duration. Such activity should not affect the quality of the user's work, the time that he dedicates to his responsibilities or the smooth operation of the service.

All information is deemed to concern the university, excluding that data which the user explicitly identifies as being private. It is thus the user’s responsibility to proceed to the storage of private data in a space designed specifically for that purpose, and to save all such data.

### *Section II.2 Continuity of service: Absences and departures*

**For the sole purpose of ensuring continuity**, the user shall inform his hierarchy of the procedures allowing access to information systems.

The user is responsible for his private data which he must destroy at the time of his definitive departure. Procedures for saving professional data will be defined in collaboration with the designated official in the institution.

## Article III. Safety Principles

### *Section III.1 Safety Rules*

The institution shall implement appropriate safeguards on the information systems available to users.
Users are advised that passwords constitute a security measure intended to prevent misuse or abuse. This measure does not confer a personal nature to the computer tools thus protected.

The type of access made available to the user is defined in terms of the tasks and responsibilities assigned to each user. The security of the information systems at the user's disposal implies that he:

- Comply with safety regulations, including rules relating to the management of passwords;
- Keep strictly confidential his password(s) and never disclose this information to a third party;
- Comply with access management, in particular, he must never use the names and/or passwords of another user, nor seek to learn this confidential information.

Furthermore, the security of resources made available to users necessitates a number of precautions:

➢ On the part of the institution:

- Ensure that sensitive resources are not accessible in the event of an absence (apart from the continuity measures implemented by the hierarchy);
- Limit access to only those resources which the user is expressly authorized to use.

➢ On the part of the users:

- If the user has no explicit authorization, he must refrain from accessing or attempting to access resources of the information system, even if such access is technically feasible;
- He must not connect directly to local networks of materials not entrusted to him or not authorized by the institution [ ];
- The user must not install, download or use, on the equipment of the institution, software or firmware without explicit permission;
- The user must comply with the systems established by the institution to fight against viruses and attacks by computer programs.

### *III.2 Duty to report and inform*

The institution shall bring to the attention of the user all information which may allow him to assess the level of risk involved in using the information system.

The user shall notify his superiors as soon as possible of any malfunction or abnormality discovered, such an intrusion into the information systems, etc.; he will also point out to the person responsible for the site any access he may have to a resource that does not correspond to his authorizations.

### *Section III.3 Safety Verification Measures*

The user is hereby informed:

- That to perform corrective, curative or progressive maintenance, the institution reserves the right to carry out interventions (if need be from a distance) on the resources available to said user;
- That all maintenance carried out at a distance will be preceded by user notification;
- That information which blocks or presents a technical difficulty of routing to the recipient, may be isolated, and if necessary, deleted.

The institution informs the user that the information system may necessitate supervision and control for statistical, tracking, optimization or security purposes or for the detection of abuse.

## Article IV. Electronic Communications

### *Section IV.1 Email*

The use of email is one of the essential elements in the optimization of work and the sharing of information within the institution.

Messaging is a tool serving educational and professional uses ; it may also be used, with moderation, for communication of a private nature.

Specific rules regulate the use of e-mailing in:

a) assigning email addresses

b) the contents of electronic messages

c) transmitting and receiving messages

d) the legal status and value of messages

e) the storage and archiving of messages

(cf. attached user guide)

### *Section IV.2 Internet*

Users are reminded that the Internet use is subject to all laws in force.

The use of Internet technology (and, by extension, the intranet) is one of the essential elements in the optimization of work as well as the sharing and accessibility of information within and outside the institution.

The institution makes Internet access available to the user whenever this is possible.

Internet is a tool for professional use (administrative and educational) and may be the medium of private communication in compliance with current legislation. In addition to these statutory provisions and with regard to the educational mission of the institution, voluntary and repeated consultation of pornographic material from the premises of the institution is prohibited.

The institution reserves the right to filter or block access to certain sites and to screen, a priori or a posteriori, all sites visited by the user as well as the corresponding access times.

Internet access is allowed only in conjunction with the safeguards put in place by the institution.

The user is informed of the risks and limitations inherent in the use of the Internet by means of training and awareness activities.

### *Section IV.3 Downloads*

All downloading of files from the Internet, including sounds and images, must be performed in compliance with intellectual property rights.

The institution reserves the right to limit the downloading of certain files which may be large or pose a risk to the security of the information systems (viruses that may affect the proper functioning of the information systems, malware, spyware, etc.).

## Article V. Traceability

The institution is legally obliged to implement a logging system * concerning Internet access, messaging and data exchanged.

** maintenance of technical information about connections such as time of access, the IP address of the user, etc.*

The institution reserves the right to develop tracking tools for all information systems, after completing a declaration with the CNIL (National Commission on Informatics and Liberties) referring in particular to the length of time that information on connections and connection times will be conserved.

## Article VI. Observance of Intellectual Property Rights

The institution reminds users that the use of computer technology implies respect for intellectual property rights as well as the rights of the user's partners and, more generally, any third party holding such rights.

Accordingly, each user must:

- use all software in authorized conditions ;
- not reproduce, copy, distribute, modify or use software, databases, web pages, text, images, photographs or other creations protected by copyright or proprietary right, without seeking the prior permission of the owners of these rights.

## Article VII. Compliance with the Data Protection Act

Users are informed of the need to comply with the legal requirements for automated processing of personal data in accordance with the law n ° 78-17 of 6 January 1978 known as "Informatique et Libertés" as amended by Law No. 2004 -801, 6 August 2004.

## Article VIII. Limitation of use

In case of non-compliance with the rules defined in this Charter and the procedures defined in the manuals, the "person legally responsible" may, without prejudice to proceedings for sanctions that may be taken against the user, limit use as a precautionary measure.

"Person legally responsible" refers to any person with the responsibility of representing the University, namely the President and his or her designees.

Any abuse for non-academic ends in the use of the resources made available to the user is punishable by the present Charter.

## Article IX. Entry into force of the Charter

This charter constitutes the rules of the institution with regard to the use of information systems.

This document supersedes all other documents or charters relating to the use of information systems.

Dijon, June 28, 2007

The University President

Sophie BÉJEAN