IT Charter

August 2019

This charter specifies the rules for the proper use of the IT resources provided. The term "computing resources" refers to the set consisting of the network, the servers and the workstations belonging to the institution, the peripherals, the software, the laptops lent to students, and access to the Internet. This charter is an appendix to the school's rules and is covered by the applicable laws:

• Law No. 78-17 of 6 January 1978, known as the law on computers and freedoms.
• Law No. 85-660 of 3 July 1985 on the Protection of Software.
• Law No. 88-19 of 5 January 1988 on computer fraud.
• Law No. 92-597 of 1 July 1992 concerning the intellectual property code.

It applies to all users of the company's information and communication systems, regardless of their status, including students, employees, temporary workers, trainees, employees of service providers, occasional visitors

1. Conditions of access to computer resources

Access to IÉSEG's IT resources is subject to authorization and may only be done as part of the user's professional or educational activities. Any other use, except when signed authorization or agreement is given by the director of the school, is strictly prohibited.

Means of access to computer resources of any kind (password, certificate...) are strictly personal and non-transferable. They will be revoked as soon as the holder no longer meets the criteria specified in the previous paragraph. In case of loss or theft, the user must contact their IT correspondent who will take all measures deemed necessary.

Except with the prior authorization of the IT Department, it is forbidden to set up computer equipment that may interfere with IÉSEG's IT resources in any way.

2. Administration of computer resources

The use of hardware or software resources and exchanges over the network can be analysed and controlled in compliance with the applicable legislation and, in particular, the law on data processing and freedoms.

IÉSEG's administrators reserve the right to take all necessary steps to assume their responsibilities and to enable the computer resources to function properly.

All Information is professional except data explicitly designated by the user as pertaining to his or her private life. As such, it is up to the user to store his or her private data in directories explicitly provided for this purpose and titled as "private".

3. Rules

Users are responsible for all IT operations, whether local or remote, made from their account. They must therefore respect the rules listed below:

<u>Account usage</u>

• Computer accounts are personal and non-transferable.
• Passwords must be kept secret.
• Identity theft in order to access IT resources is punishable with sanctions.
• The computer has to be locked when leaving the post.
• Inform the IT Department of any suspected violation, or tentative of violation, of your computer account.

<u>Use of hardware resources</u>

• Do not try to change the configuration of workstations or laptops loaned out or made available.
• Take special care with all hardware.
• Do not try to edit or delete network data.
• Do not deliberately disrupt the operation of the services and do not use programs to circumvent security or introduce harmful programs (viruses, spyware or other).
• All anomalies (hardware / software) must be reported to the IT department.
• The institution cannot be held responsible for the disappearance of data. (files, programs, reports, etc.) hosted on the equipment.
• Always make backups

Use of personal laptops

• Installation of an anti-virus is mandatory.
• Security update of the anti-virus and the operating system is mandatory.

Use of messaging services

• The use of messaging services is primarily intended for professional use.
• Do not open message(s) from suspicious sources.
• Do not forward personal data files to an external addressee out of the exchanges planned.
• Limit the personal data exchanges by email. Privilege the deposit on shared secured spaces.

Use of Internet / Intranet services

• Viewing websites with illegal content is strictly prohibited.
• Downloading (programs, videos, music...) is strictly prohibited.
• Dissemination of information via the Internet must comply with the law; this implies, among other things: respect for copyrights (musical excerpts, literary excerpts, photography, etc.), privacy, the right to image, do not disseminate unverified information or illicit information

Use of the trading room

•The creation of BLOOMBERG PROFESSIONAL user accounts is strictly limited to IÉSEG students and staff.

• Do not give your BLOOMBERG PROFESSIONAL access codes to other persons and do not allow outsiders to enter the trading room.
• Only a limited amount of data can be extracted by the user within the exclusive framework of teaching and research within IÉSEG. Do not share data with third parties and do not store this data on external media.
• Do not look for additional paid services or transactions through the platform.

Service “Le Wagon”

The use of LE WAGON user accounts is strictly limited to IÉSEG students and staff. It is strictly forbidden to communicate your access to other users.

Use of personal data

We understand by personal data all data referring to an identified or identifiable person (candidates, students, employees, interns, companies’ contacts, providers, visitors…)

• Any new processing of personal data must be declared to your manager in order to be documented.
• Do not multiply reference sources for personal data, centralize them instead.
• Limit the extractions of personal data
• Do not forward files with personal data to external addressees out of the exchanges already planned
• Do not incorporate external data files out of the expected exchanges
• Limit personal data exchanges through non-secured means (paper, non-secured messaging…) Privilege the deposit on shared secured spaces.
• Do not conserve personal data beyond the time required.
• Stock documents, files… containing personal data in a secured place.
• Do not leave documents containing personal data on the printers.
• After using them, throw away documents containing personal data in secured bins or destroy them in shredders.

4. Penalties

In the event of a breach of the rules set out in this charter, the IT Department reserves the right to immediately remove, for an indefinite period, all or part of the offender's access to IÉSEG's IT resources.

I acknowledge having read the school's computer charter and have been informed of the arrangements made (checks made when logging in, monitoring the use of the various workstations) to guarantee proper use of the educational resources belonging to the school.