USJ 1875
Université Saint-Joseph de Beyrouth
جامعة القدّيس يوسف في بيروت

Charter for the Use of Saint Joseph University of Beirut IT Resources and Information System

(The French text of this Charter was approved by the University Board at its 200th meeting on June 19, 2019)

Introduction

The present Charter establishes the rules for the use of IT resources and the Information System of Université Saint-Joseph de Beyrouth (USJ - Saint Joseph University of Beirut) hereinafter referred to as "the University". It defines the respective duties of the users and of the University. It applies to all computers, whether fixed or mobile, shared or personal.

Its purpose is to raise awareness among users of the risks associated with the use of IT resources, especially in terms of data confidentiality. It urges all interested parties to handle these resources with caution. In particular, it recalls that the use of IT must be consistent with intellectual property rights.

The IT resources in question are those that the University makes available to users within the framework of their professional activity. These resources include the Information System, i.e. all the hardware, software, databases or telecommunications networks made accessible to users.

Such access must be fully respectful of collective and individual freedoms. In particular, it safeguards privacy, personal data and property. It also abides by the Lebanese legislation, as well as the regulations of Saint Joseph University of Beirut.

The present Charter, as well as any subsequent amendment, comes into force as of its adoption by the University Board.

All users of the University's IT resources and Information System must be informed of this Charter and must sign it.

1. User Obligations

1.1. General Obligations

In addition to the obligations associated with their employment status or contract, the user shall be subject to the following general obligations:

1.1.1. The user is held responsible for the use of the University's IT resources and Information System.

1.1.2. The user is prohibited from spreading hateful or defamatory messages, or any form of advocacy of crime, racism, etc.

1.1.3. The user shall not duplicate, distribute or alter software, databases, web pages, texts, photographs or any other work protected by copyright, without the consent of the copyright owner. The user must also comply with trademark law.

1.1.4. The user is obliged to treat correspondence, information and documents to which they may have access with caution and confidentiality.

1.1.5. Upon final leave from the University, the user shall lose their right to access IT resources, including WiFi, and the Information System.
The University may, however, keep the user's e-mail address (@usj.edu.lb or @net.usj.edu.lb); the user then undertakes to respect this Charter even after leaving.

1.2 Special Obligations

1.2.1. Obligations associated with the professional nature of the user's activities
The IT services of USJ are restricted to professional activities, i.e. teaching, research, administration and service operations of the University.

a. The user must guarantee access at all times, even in their absence, to their business data when such data are related to the administration and service operations of the University.
Access to business data related to collective research activities is subject to conditions established by the laboratories and research centers involved.

b. Occasionally, the user may make private use of their workstation, provided that it does not serve any profit-making purpose. The user is solely responsible for the personal data saved on their workstation; they must delete it upon leaving, otherwise the University reserves the right to do so.

c. If the user accesses social networks from the University's IT resources, the user must comply with the Charter for the Use of Saint Joseph University of Beirut Social Networks.

1.2.2. Obligations associated with computer security
For security reasons, the user must:

a. Lock the personal or shared workstation after use.

b. Refrain from disclosing passwords to third parties, including their supervisor, unless there are compelling reasons to do so.

c. Refrain from downloading or installing, on their professional workstation, free or paid software or software packages, with the exception of express authorization from the University.

d. Rely on the tools and means of data backup made available by the University. The user shall not upload data on a server open to the general public (Google, Yahoo, etc.) if not authorized by the competent officials.

e. Refrain from retrieving business data and using it, off University premises, without prior authorization.

f. Notify their supervisor or the Chief Information Security Officer of any attempted breaches or other unusual occurrences on their account.

g. Comply with the University's designated anti-virus and cyberattack measures.

h. University guests may access the Information System only with the prior approval of the IT Resources Administrator.

2. University Obligations

2.1. General Obligations

2.1.1. The University shall guarantee the proper functioning and security of the networks. It shall carry out this mission in compliance with the legislation and regulations in force, in particular those relating to the protection of personal data and respect for private life.
2.1.2. It shall inform all those involved of its security policy, as well as of the rules for the proper use of IT resources and the Information System.
2.1.3. It shall conduct information and training sessions on the use of IT resources.
2.1.4. It shall provide each user with their own "username and password".
2.1.5. The University may require interventions on the user's workstation in order to maintain network security. These interventions shall be announced to the user who must be informed before applying them.
2.1.6. IT network administration and maintenance may result in the collection of statistics requiring user identification. Users will be informed in advance by the University. Staff in charge of data collection are bound by professional secrecy.
2.1.7. The University shall appoint one or more IT resources and Information System administrators.

2.2. Administrator Obligations

In addition to the obligations imposed on any user, the administrator shall also be subject to the following obligations:

2.2.1. The administrator shall provide users with access to IT resources and Information System modules and shall ensure that they work properly.
2.2.2. The administrator shall respect the rights of the user, in particular their personal freedoms and their private life.
2.2.3. The administrator shall protect the confidentiality of the data at their disposal, in particular those of a private or confidential nature that they may encounter in the course of their work.
2.2.4. The administrator shall comply with the rules of professional ethics and deontology.
2.2.5. The administrator shall establish records to ensure continuity of service upon their final leave from the University.
2.2.6. The administrator shall ensure information security. To this end, they shall:
   a. Ensure that users comply with security guidelines.
   b. Filter or prohibit access to certain sites, as well as certain downloads of files, should they be deemed a security risk to the University's Information System.
   c. Take prompt action when they are aware of illegal actions or illicit data on IT equipment.
   d. Notify their supervisor and the Chief Information Security Officer immediately of any security incident, irregularity, vulnerability or malfunction.
   e. Keep their own password strictly confidential, unless required to ensure continuity of service and duty.
   f. Conduct a periodic audit of all access to the University's IT resources and Information System. This audit shall identify attempted breaches of the IT system and assist in identifying potential liability.
   g. When maintenance or monitoring activities of IT resources require the administrator to access all user data, they shall handle all data with absolute confidentiality and shall respect the private property.

3. Sanctions

Without prejudice to any disciplinary or legal proceedings that may be taken against offenders, the University may suspend access to IT resources and the Information System for any user who infringes the provisions of this Charter.

Annex to the Charter for the Use of IT Resources and the Saint Joseph University of Beirut Information System

Definitions

Administrator: Any person, staff member of the IT Department (STI), who is explicitly assigned to the development, operation, maintenance and monitoring of the use of the University's IT resources and Information System, and who has specific and privileged access rights in this respect. In the course of their work, the Administrator may have access to information about other users or their activities, as well as to confidential information sources.

Mobile devices: Mobile equipment that allows remote access to the University's IT resources, including cell phones, tablets, and laptops.

Data: Any information available in different formats (database, files, printed documents, emails, etc.).

Security policy: Set of guidelines and procedures aimed at protecting the University's IT resources and Information System.

IT resources: All hardware and IT or digital equipment that can be provided to users in the course of their professional activity.

Information System security: All technical, organizational, legal and human resources put in place to maintain and guarantee the security of IT resources and the Information System.

Information System: Set of integrated IT modules used as a management tool for the University.

User: Any person, regardless of employment status, who has continuous or occasional access to the University's IT resources or Information System in the course of their professional activity, whether by means of fixed or mobile devices. Users include:

- Any administrative staff member, whether tenured or non-tenured;
- Any teacher, whether tenured or non-tenured;
- Any student or intern;
- Any researcher or PhD candidate;
- Any University guest;
- Any contractor having been hired by the University;
- Any administrator;
- And more generally, all individuals using the University's IT resources, as well as those having remote access to the University's network.

Applicable Provisions

- Preamble of the Lebanese Constitution of September 21, 1990 Relating to the Respect of Private Life.
- Law no. 75 of April 3, 1999 Relating to the Protection of Literary and Artistic Property.
- Law no. 81 of October 10, 2018 Relating to Electronic Transactions.
- Law no. 28 of February 10, 2017 Relating to the Right of Access to Information.
- Criminal provisions: Article 579 et seq. of the Lebanese Criminal Code.
- Charter for the Use of Saint Joseph University of Beirut Social Networks.

Last Name .....

First Name .....

Position .....

Institution .....

Read and approved (Signature) .....

Date .....