Charter for the Use of ITQB Computing Resources

(Adapted from the charter for use of computing resources of the European Synchrotron Radiation Facility)

Contents

1. Introduction
2. Definitions
3. Basic principles
4. Personal use of the ITQB computing facilities
5. Users rights and duties
5.1. Users rights
5.2. Users duties
6. Rights and duties of the system and/or network administrator
6.1. Network administrators rights
6.2. Network admnistration duties
7. Rights and duties of the management
7.1. Rights of the management
7.2. Duties of the management
8. Sanctions

1. Introduction

The present charter defines the rules for the use of ITQB computing facilities.
Its contents are communicated to all new users of ITQB computing facilities, at the moment they are given an ITQB e-mail account.
The charter is part of the ITQB Internal Regulations Booklet made available to all members of the staff and collaborators.

2. Definitions

"ITQB computing facilities":

a) all PCs (Personal Computers including those which are self-service), laptop computers, workstations, servers, and peripheral systems such as printers, directly or indirectly connected to any ITQB computing and/or telecommunication networks;

b) all support utilities, program libraries, applications and other software packages, as well as all documentation, electronic mail, Web, and intranet services installed or running on any of the computers and making use of the above-mentioned networks.

"Users": any person making use of ITQB computing facilities.

"Management": the members of the ITQB Direction or any other staff member appointed by the Director.

"System/network administrator": any member of the ITQB staff individually appointed as the responsible for the operation and security of the ITQB computing facilities.

3. Basic principles

ITQB computing facilities shall be used in accordance with ITQB objectives. Their use is part of the professional duties of the users as defined by the management. Personal use of the ITQB computing facilities is tolerated to a certain extent, as specified in Section 4.
ITQB endeavors to maintain and protect its computing facilities. It cannot, however, guarantee their proper functioning or perfect confidentiality of the information stored.

4. Personal use of the ITQB computing facilities

The personal use of ITQB computing facilities is tolerated, provided that:

a) it is in compliance with the present charter;
b) it is not detrimental to official duties, including those of other users;
c) the frequency and duration are limited and there is a negligible use of ITQB resources;
d) It does not constitute a political or commercial profit-making activity;
e) it does not violate applicable laws.

In case of conflict on the application of these standards, the Director of ITQB will have the final decision.

Ultimately, personal use of ITQB computer resources is the sole responsibility of the user. It is therefore up to each user to save and protect his/her personal information against risk of loss or violation.

5. Users rights and duties

5.1. Users rights

Users shall have the right to be informed about the proper use of their computing equipment, and as far as possible about the inherent safety and security problems. Additional information and recommendations are available on the Intranet. If need be, the system and/or network administrator can be consulted.

5.2. Users duties

Concerning ITQB interests:

a) should the user have access via computing facilities to confidential information, he/she must respect such confidentiality;
b) the users shall respect the integrity and confidentiality of data belonging to the ITQB;
c) computing resources must never be used to undermine the image of the ITQB.

Concerning the security of the ITQB system and network:

a) it is forbidden to voluntarily perturb the ITQB computing facilities;
b) users must respect the technical and security advice supplied by the system and/or network administrators or by the management (e.g. protection against viruses);
c) it is forbidden to seek unauthorized access to accounts;
d) it is forbidden to look for, disclose or exploit any security weakness in the ITQB computing facilities or use these facilities to do so.

Concerning the security of the users:

a) the users must protect their personal computer or workstation against unauthorized access. They shall also protect their personal account by avoiding obvious passwords. If necessary, they shall seek the advice of the system and/or network administrator;
b) it is forbidden to disclose passwords to any third party, unless absolutely necessary for professional reasons;
c) upon request from a system and/or network administrator, users shall select a new password;
d) it is forbidden to use a third party account and password, or to act in an anonymous manner;
e) users shall respect the privacy of other users' information. It is forbidden to change, modify, falsify and/or distribute information belonging to another user.

Concerning the use of computer resources:

a) users shall respect the proprietary rights related to the ITQB computing facilities, (including software copyrights). In particular, all users must be in possession of the appropriate license for all software used;
b) users shall use ITQB computing resources in a way that will not impede the work of other users or their access to the network. If such a work is likely to overload the network, users must ask the network administrators for a previous approval;
c) if users have been given an account with privileged access in connection with specific professional duties, they shall inform the system and/or network administrator as soon as those duties no longer require privileged access.

Concerning the use of the Internet:

a) it is against the law to use ITQB resources to load, consult, stock, or distribute documents or information liable to undermine the respect of the human being and his dignity. In particular, this applies to documents of pedophile or racist nature, or documents that undermine the integrity of the individual by violating the secret of correspondence, threat, insults, harassment, etc.;
b) this also applies for usages that attack property, especially fraud and offences under the Intellectual Property Rights legislation (http://www.gda.pt/legislacao_codigo_intro.html);
c) personal Web-pages are authorized only if they are linked to the professional activity (e.g. CV, scientific publications).

Concerning the use of E-mail:

a) unauthorized access to, or forgery of e-mail is forbidden;
b) spamming is forbidden. E-mails sent to more than 20 addresses (unless it is for professional use), chain messages (messages received individually in the context of collective dispatches asking to forward them collectively) and wide distribution of advertising messages inside and outside the ITQB can be considered as spam.

6. Rights and duties of the system and/or network administrator

6.1. Network administrators rights

The system and/or network administrators are in charge of the normal functioning and security of the network and systems.
They are allowed access to information in ITQB computing facilities in order to:

a) solve problems affecting ITQB computing facilities, such as viruses, etc., perform upgrades and install new facilities;
b) detect computer security weaknesses or computer security violations or attempts to violate the computer security;
c) monitor available resources to ensure the adequacy of ITQB computing facilities;
d) investigate, upon written orders from the Director, in case of a suspected infringement of this present charter by a user;
e) remove accounts when a user's contract with ITQB is terminated.

On a regular basis, system and/or network administrators use the following tools to monitor the e-mail and Web traffic:

a) storage of the Web links consulted (including the computer name of the client, the site name, time, and file size);
b) daily compilation of Web statistics (the top ten ITQB computers using the Web and the top ten Web sites visited);
c) storage of e-mail exchanges: time, size, sender, and destination (not the contents nor subject).

The system and network administrators may only exploit the information to which they have access with the purpose of ensuring good functioning and security of software applications.

6.2. Network admnistration duties

System and/or network administrators have the obligation to report computer security problems, as well as any serious indications of ill use of computing resources to the direction of ITQB.

The system and network administrators must respect an obligation of confidentiality towards the users, in particular concerning the contents of the information they may have acquired.

Any personal information susceptible to be acquired by the system and/or network administrator must be dealt with under confidence.

The administrators are exempted of their obligation of confidentiality in two cases:

a) upon a written request from the Director of ITQB, when correct functioning of the systems and/or the interests of the ITQB are in peril;
b) whenever the application of legal and regulatory provisions implies the disclosure of information.

7. Rights and duties of the management

7.1. Rights of the management

a) in case of serious indications of ill use, the Director of ITQB can ask the administrator to carry out a control of the computing equipment. The user will be asked to be present during the operation;
b) the Director can also deposit a formal request at the competent official instance for an authorization to have computer traces or data seized.

7.2. Duties of the management

Management must ensure that the present charter is known and applied by all staff members and collaborator of ITQB.

8. Sanctions

Disrespect of the present charter may result in:

a) Suspension or suppression of the access to the computer facilities;
b) disciplinary sanctions;
c) civil liability or criminal responsibility for damages he may have caused including the non-respect of confidentiality rules as referred to in Section 6.