IT CHARTER

Révisée le 7 janvier 2014

SECTION 1 1
Preamble 1
Scope of application 2
SECTION 2 2
Rules of good practice 2
SECTION 3 4
Systems Administrators 4
SECTION 4 5
Accounts and passwords 5
SECTION 5 6
Security 6
SECTION 6 7
Instant messaging system 7
SECTION 7 8
Privacy and personal data 8
SECTION 8 9
Software and copyright 9
SECTION 9 9
Applicable Sanctions 9
SECTION 10 10
Règles de publication – Dépôt – Entrée en vigueur 10

SECTION 1

Preamble

Computer security in the Institute is an objective that must be shared and that can only be achieved in a climate of loyalty and mutual trust.

The purpose of the present IT Charter is to define rules concerning the use of computer means and systems at ETSI[1]. This IT Charter therefore falls within the framework of laws in force.

The constant progress of information processing and communication techniques increases the need to specify rules to protect the private life of employees in the ETSI Secretariat while maintaining the prerogatives of systems administrators[2] and security within the Institute.

This Charter is applicable to all ETSI IT services users.

This charter replaces the previous charter which was in force and annexed to the ETSI Personnel Internal Regulation.

[1] The terms ETSI or European Telecommunications Standards Institute shall mean the ETSI Secretariat including consultants, trainees and sub-contractors, and representatives of ETSI members and non-members.
[2] The terms Systems Administrator shall mean any person with special access rights to computer systems (PCs or servers), special rights to change the security rules, special rights of access to passwords or rights to change the access rights to central databases.

Révisée le 7 janvier 2014

Introduction

The rapid development of Information Technology and digital networks within firms and throughout the world constitutes extraordinary collective wealth but has revealed both abuse and weaknesses that cannot be ignored.

Thus, there are many computer crimes, among which computer system intrusion via a network, illegal copies of software or files not copyright free, borrowing of a third person's identity, attempts at these offences, conspiracy to commit them, destruction of information belonging to others, voluntary corruption of the operation of the computer system, etc.

The ETSI Secretariat, a user of computer facilities and networks and a provider of services to its Members, clients and partners, is also subject to potential risks and must enforce the laws in the field.

Compliance with the rules is the inevitable price to pay for freedom in communication and use of computer means.

The user shall be held personally liable for failure to comply with the IT Charter of ETSI which may be directly or indirectly detrimental to all or part of the Institute.

The Institute is itself subject to rules governing the proper use of computer means, and must therefore uphold both the code of good practice and the law.

Security will be achieved if everyone abides by the rules and is vigilant.

Scope of application

The rules and obligations set forth below apply to any person, regardless of his or her status, authorized to use the Institute's computer facilities.

The facilities shall mean computer systems or means, servers, workstations, terminals, micro-computers installed in offices, in meeting rooms and public areas, portable micro-computers, the mobile computer equipment that may be lent out occasionally or any other hardware (printer, scanner, etc.) used in the operation of the Institute.

Compliance with the rules defined by the present IT Charter also applies to the use of computer systems of independent organizations as well as systems that can be accessed by telephone or digital networks.

SECTION 2

Rules of good practice

1. The IT Charter of ETSI is a set of rules of good practice that must be complied with. It aims to inform and warn users of the risks involved.
2. The IT means of the Institute are to be used exclusively for the performance of the professional tasks for which they are designed. As a consequence, any file or email

stored or transferred via the IT means of the ETSI is deemed to be of an exclusively professional nature and as such, cannot be considered as private.

3. Save prior authorization granted by the managers concerned, these means may not be used to carry out projects that are not part of missions entrusted to the users.
4. Using the IT means of the Institute for personal purposes is nevertheless authorized on an exceptional basis, for urgent needs. In such cases, the user should specify the personal nature of the file or the email, and promptly destroy any incoming or outgoing personal messages or files or otherwise keep them in an identifiable personal folder. On no account should such messages or files be kept in their inbox or outbox. .
5. Participation in games on the network, on-line lotteries, non-professional data exchanges in point-to-point mode, paid Internet connections and other recreational or pecuniary applications are forbidden.
6. Data conveyed or put on the network by network users must be legal. Therefore, users must abide by all legal provisions.
7. Each user agrees to take care of the hardware and computer rooms provided to him or her and to inform the IT Department of any anomaly noticed.
8. In the event of a foreseeable absence equal to or longer than half a day, each user agrees to activate the automatic absence message function beforehand.
9. In the event of an unforeseeable absence equal to or longer than half a day, the relevant employee's line manager reserves the right to ask the IT Department to activate this automatic message and/or the redirection of all their messages to another mailbox.
10. Each user agrees to store in a place shared by the relevant employees the messages or files required for their job to be continued in the event of their absence. Otherwise, in the event of an absence equal to or longer than half a day and in the event of an urgent business need, the relevant employee's line manager reserves the right to ask the IT Department to give temporary access to another user so that he may retrieve the messages or files needed to ensure business continuity.
11. Each user must monitor the use of his or her disk space on the network (files and mailbox) to strictly occupy the disk space necessary for his or her work. As a result, disk storage quotas may be implemented by the systems administrators, frequent cleaning may be demanded, as well as compression and archiving in compliance with the instructions transmitted by the IT Department.
12. Users must make optimum use of file archiving and compression means that they have.
13. Activities that might take up a lot of computer facilities (printing large documents, substantial calculations, intensive use of the network or mailbox ...) must be carried out at times that cause the least amount of disturbance to the community.

Each user agrees not to:

1. intentionally carry out, attempt to carry out or cause to be carried out any operations intended to harm a person, a group, the ETSI or another establishment,

2. intentionally change or destroy information on one of the systems connected to the network,
3. intentionally interrupt the normal operation of the network or of one of the systems connected to the network,
4. connect or attempt to connect to a protected site without authorization,
5. attempt to read, copy or disclose data protected by another user,
6. change another user's data without having explicit authorization to do so,
7. conceal one's true identity,
8. appropriate another user's password,
9. spoof machine names (micro-computers or servers) addresses, or identities
10. intercept or attempt to intercept communications between third parties,
11. connect peripherals or computers such as storage units or personal laptops to the ETSI internal network without a prior authorization from the IT Department.

SECTION 3

Systems Administrators

Responsibilities

1. ETSI's servers and networks are managed by systems administrators that are responsible for the proper operation thereof and the quality of the service provided within the limits of the means allocated.
2. Despite the backups made regularly, the restore of files is not guaranteed even if the systems administrators must do their utmost to retrieve lost files.

Duties

In accordance with the means at their disposal, they are required, above all

1. to enforce the rights and responsibilities of users,
2. to respect, when they are themselves users of computer systems, the rules that they impose on other users,
3. to inform their superiors of any non-compliance with the present IT Charter,
4. to respect and uphold the confidentiality of files, emails and any data under their responsibility,
5. to ensure the security and confidentiality of the networks by using all the technical and human resources required,

6. to inform users, as far as possible, by all appropriate means, of any intervention likely to disrupt or interrupt the ordinary use of the computer facilities,
7. to keep interruptions in computer services to a minimum and to choose dates and times that are the least detrimental to users,
8. to cooperate with the security agents of independent networks in the event of a security incident involving a server they administrate

Rights

So as to mitigate a possible incident in operation or security, the systems administrators may

1. take conservatory measures,
2. stop the execution of any IT process or service,
3. remove rights of access and passwords,
4. close a network to the outside world,
5. stop any server.

The need to act, as an exception, on the services, data and communications must be justified by an urgent collective need assessed by the superiors or, in an emergency, directly by the systems administrators.

SECTION 4

Accounts and passwords

1. The network accounts are created and closed by the IT Department. They are temporary, strictly personal and non-transferable. They shall disappear when the holder leaves the Institute.
2. They are composed by a username (unique), an initial password (that must be modified by the user) and a set of permissions.
3. They are disclosed to a new user once he or she has been informed of the existence of the present IT Charter.
4. The systems administrators may, with or without giving notice, take the necessary steps against any user (including temporarily closing his or her account) who disrupts the smooth operation of the computer facilities or who fails to comply with the rules set forth in this document. User may contact the Manager responsible for the IT Department or the Management which may take the appropriate actions to resolve the problem.
5. The passwords must not be disclosed to a third person, including the systems administrators. A right of access may be transferred, if need be, to another user for

service-related reasons after notification by the systems administrators to the Managers concerned. As a general rule, the Manager (or a person appointed thereby) is responsible for informing the systems administrators of any changes concerning the right of access of a user such as temporary transfer of the right of access (absence, leave,…), change of function leading to a change in the right of access, change in the civil status at the user's request, removal of an account etc.

6. The passwords must respect the requirements of complexity and length which are defined by the IT Manager.
7. The passwords must be changed regularly, according to a periodicity and an history defined by the IT Manager.
8. An automatic mechanism will be installed obliging users to respect the requirements of complexity, length, periodicity and history.

Each user agrees to:

1. contribute to security on a personal level; each user is responsible for the computer operations, both local and remote, conducted using his or her account,
2. be responsible for changing his or her initial password,
3. choose a new password that must follow the requirements of complexity and length stated by the IT Manager,
4. change the passwords regularly and particularly after a demonstration or a presentation in public,
5. take the necessary steps, in the event of absence, to make the data under his or her responsibility accessible,
6. immediately inform the systems administrators if his or her password no longer allows him or her to connect, if he or she suspects attempted or actual piracy of his or her account.

SECTION 5

Security

The user must take the necessary precautions to:

1. keep his or her password secret,
2. protect his or her files,
3. normally end his or her sessions of connections to computer facilities,
4. lock access or disconnect his or her workstation from the network,
5. keep in a secured place any digital media which might contain confidential, professional or personal data,

6. to protect data that guarantee compliance with the confidentiality undertakings made by the Institute to third parties.

Each user agrees

1. that cryptography, to ensure the confidentiality of data, may not be used to conceal information that breaks the code of good practice established by the present IT Charter,
2. not to introduce viruses intentionally and to strive to avoid the spread thereof through the computer means,

   In order to ensure the security of the IT systems, the IT Department must be informed in case of doubt concerning the transmitter, the content of a message or an appended file. The IT Department must be immediately informed if a virus is detected or an anomaly noticed in a mail or an appended file. When a virus is detected, the email must not be opened by the recipient and must be immediately destroyed.
3. not to research into the security of the IT systems without prior authorization from the systems administrators,
4. not to download, develop, install or copy a software tool to circumvent security, saturate facilities, illegally open a communication port, circumvent software protection, decrypt passwords, pick up information on the network etc.
5. not to make use of any holes in security or anomalies in operation,
6. to inform the systems administrators of any holes in security and to refrain from advertising such information.

SECTION 6

Instant messaging system

1. Instant messaging system is an additional method of communication which can be used within the Secretariat.
2. Instant messaging system is not intended to replace electronic mail (email).
3. Each user will be attributed an account in the instant messaging system by the IT Department, to perform his/her professional activity.
4. During his/her connection to his/her professional computer, each user must be connected to the instant messaging system.
5. This tool permits each employee to know if a colleague can be contacted by viewing the presence status, which shows the level of availability.

6. It is mandatory to have the presence status visible to all employees of the Secretariat.

7. Users must maintain the information which allows others know if they are working outside of the ETSI premises.

8. The choice is left to the user whether or not to archive his/her conversations in his/her own storage area. The IT Department does not store the conversations under any other storage area or network drive.

9. Users are authorized to connect to another instant messaging system in order to contact people outside the Secretariat who cannot be contacted through the system put in place by the IT Department.

SECTION 7

Privacy and personal data

Users are informed that the systems administrators, as part of their work,

1. have specific rights to access any stored or circulating on the ETSI networks. They agree only to use them for the proper operation of the computer facilities according to the terms stipulated herein,
2. may keep for history all connections to the network, access to the Internet, messages sent and received, access to databases and changes to data in the event of a security problem or system malfunction,
3. may archive these journals (log files) for a maximum term of 3 months. They are not examined unless there is an absolute necessity to do so for security reasons or due to system operation. The decision to examine such information may be made as part of a legal enquiry,
4. may keep for history the nominative data for a maximum term of 3 months. They may be consulted only when required by law or for history purposes,
5. may monitor work sessions in progress if they suspect failure to comply with the IT Charter or in case of technical problem,
6. may compress or move, with or without giving notice, any files considered to be excessive in size or delete, after giving notice, with the owner's agreement or decision from the Manager,
7. may move, with or without giving notice, any files without a direct link to the professional use of the computer system or delete, after giving notice, with the owner's agreement or decision from the Manager,
8. reserve the right to change the priority of a task or to stop the execution thereof in the event of abusive use of the facilities, after notifying the user concerned if possible.

Users are informed that :

1. Data processing of personal information shall be conducted in full compliance with the provisions of the law.
2. The right of privacy of each person shall be respected.
3. The publication of personal photographs on the public domain (Internet) requires the express consent of the person involved.
4. The possibility of reading a file does not grant authorization to read it.
5. General laws prohibit the following types of information or message: insulting or abusive, pornographic, paedophiliac, slanderous, incitement to racism or xenophobia, attack on human dignity.

SECTION 8

Software and copyright

Users must not under any circumstances,

1. download, install or copy any software on an ETSI computer, including software that is part of the public domain or make such software accessible on the network, without obtaining an explicit prior authorization from the IT Department,
2. duplicate protected software,
3. copy an application developed by the ETSI Secretariat without prior authorization,
4. export all or part of the source codes of applications outside the ETSI buildings,
5. circumvent the restrictions of software use.

SECTION 9

Applicable Sanctions

1. Laws and regulations define the sanctions applied to those who misuse computer means.
2. Any user who does not abide by the law may be prosecuted and punished in the manner provided for by legislative texts in force.
3. Criminal sanctions do not bar disciplinary sanctions.

4. Any user failing to comply with the rules and obligations defined in this IT Charter is liable to disciplinary sanctions provided for by regulatory texts in force.

SECTION 10

Règles de publication – Dépôt – Entrée en vigueur

The present IT charter has been :

- Submitted to the CHSCT on 17 December 2013
- Submitted to the “Comité d’Entreprise” on 18 December 2013.
- Communicated to the Labour Inspector on 7 January 2014
- Deposited at the Grasse Labour Court Secretariat on 7 January 2014
- Posted-up at the work premises on the panels reserved for the Directorate on 7 January 2014.
-

It will come into force on 7 February 2014, one month minimum after the accomplishment of the last formality described above.

It is annexed to the ETSI Personnel Internal Regulation of which it is considered to be an integral part.

Drawn up at Valbonne
On 7 January 2014