CHARTER FOR USERS OF COMPUTER RESOURCES AND COMMUNICATION NETWORKS

POLICIES AND PROCEDURES FOR NORTH AMERICA

FOREWORD

The use of computer resources and communication networks is a major factor in the growth of companies in the Saint-Gobain Group.

Indeed, these work tools deliver quicker and more effective access to more information, and offer improved communication with a company’s partners.

For the company and its users their security and reliability should be a priority and on-going concern.

Similarly, protection of confidential data, compliance with current legislation, especially with regard to intellectual property and electronic data processing, together with company loyalty, are all part of the duties and responsibilities of every user.

The aim of this Charter is to remind everyone of these obligations and to set out for users the relevant rules in these areas.

Without question, safeguarding the corporate industrial, commercial and financial interests of the Saint-Gobain Group, and also our corporate image, is dependent on compliance with these regulations and the proper use of the various technologies.

This Charter applies to all company employees who, in the performance of the tasks assigned to them, must organize, install, modify or use, either directly or indirectly, computer resources and communication networks.

It equally applies to all persons who, while not company employees though engaged in work for the Group, must organize, install, modify or use, either directly or indirectly, its resources and networks; for example, trainees, customers, suppliers, subcontractors, agency workers, outside personnel, consultants, etc.

The relevant departmental supervisor should therefore notify these persons of the existence and content of the Charter.
THE USE OF COMPUTER RESOURCES AND COMMUNICATION NETWORKS IS RESTRICTED TO PROFESSIONAL PURPOSES

Computer resources: individual desktop or laptop computers, personal digital assistants, servers, etc.; data communication networks: internal IT networks, internet, etc. and telephone systems: digital telephones, faxes, mobile phones, etc. are the work tools the company makes available to users to help them perform their tasks.

These computer resources and communication networks are therefore limited to professional use only (Except for inconsequential, occasional non-professional use, provided that such non professional use (i) does not unduly interfere with the user’s tasks, (ii) does not expose the network to a risk, and (iii) that the user commits to respect security rules as set forth in the present Charter). Company cannot be held liable for any consequences coming from such personal use.

The user is responsible at all times for the use he or she makes of the company’s computer resources and communication networks, and should comply with the guidelines in this Charter.

Consequently, the company cannot be held liable for any infringements committed by users who are in breach of these regulations.

PROTECTING THE SECURITY OF COMPUTER RESOURCES AND COMMUNICATION NETWORKS

1. General rules

Protecting the security and integrity of computer resources and communication networks is a priority and is part of users’ responsibilities.

Under no circumstances should users engage in the following specific acts or activities:

- Load, store, publish, disseminate, distribute or use, through the medium of the company’s computer resources and communication networks, any documents, information, images, videos, etc. liable to adversely affect:
  - The company's computer resources and communication networks, and, more specifically, the integrity and storage of the company's and/or the Saint-Gobain Group's data.
  - The company’s and/or the Saint-Gobain Group’s internal and external corporate image.
  - Respect for people and human dignity, as well as the protection of minors, through the use of materials which are violent or pornographic in character, against public decency, defamatory or libelous, or in general terms unlawful.
  - The construction and/or implementation of computer programs designed for these purposes, as well as access to web servers dealing with such subjects are also prohibited.
  - Users should refrain from any behavior likely to induce a third party to send them the types of documents identified above, in whatever form.
  - Should users happen to receive such documents, they should destroy or delete them immediately.
CHARTER FOR USERS OF COMPUTER RESOURCES AND COMMUNICATION NETWORKS

POLICIES AND PROCEDURES FOR NORTH AMERICA

- Use the company’s computer resources and communication networks in order to harass, threaten or insult persons.

- Copy software, or introduce or themselves install any software or equipment whatever, which is protected by laws on intellectual property, without first requesting and obtaining authorization from the person in charge of IT Security. Users shall refrain from asking third parties to send them enclosures of such programs, software, software packages, etc.

- When accessing external mailboxes knowingly download or open dangerous enclosures like .exe, .com, .scr etc…. In case of doubt, users shall ask their mail administrator or help desk.

- Knowingly load or send any files containing viruses or corrupted data.

- Falsify the source of data contained in a file.

- Send mass messages (more than 20 addressees, excluding the use of company mailing lists for professional reasons) or chain messages (messages received individually as part of a mass distribution of mail with an invitation to forward messages in the same way).

- Use the company’s resources in such a way that other users’ access is hampered.

- Conceal their identity when using their account.

- Use an account other than their own. Users should immediately notify the local IT Security Officer or Helpdesk of any attempted violation of their account and, more generally, of any anomaly observed with regard to the use or operation of computer resources and communication networks.

- Without prior authorization, modify any information sent to them if doing so is not within the scope of their tasks, obtain knowledge of any information not intended for them, or copy, modify or destroy such information.

- Request greater rights of access or use than those required to perform their tasks.

- Communicate passwords of “administrator” accounts to persons who have no need of them to perform their tasks.

Employees are reminded that some of the acts and activities listed above can constitute criminal offences.

The company reserves the right to carry out regular checks and controls within the scope and terms of the law (see Appendix 1)
2. **Security measures for the protection of computer resources and communication networks**

To enable the company to achieve first-rate protection of computer resources and communication networks users should as a minimum respect the following requirements:

- Always make use of passwords for systems and applications that include that capability even if not technically enforced.
- Change passwords regularly, even if not automatically requested to do so. Avoid passwords which can be easily discovered, such as nouns, first names, dates of birth, simple series (123456), etc.
- Never lend out their login/password. This is, however, allowed for maintenance work. Wherever possible, the owner of the account should always type in his or her password.
- Never allow outside persons access to their workstation, especially remotely, without the prior express authorization of the person in charge of IT Security.
- In particular protect confidential or secret files belonging to the company and/or the Saint-Gobain Group.
- Use antivirus software for all documents originating outside the company.
- Do not deactivate antivirus software at workstations (desktops or laptops) and servers; do carry out regular antivirus updates whether automatic (network) or voluntary (laptops), and in the event of virus alerts.
- Do not cancel sleep mode requiring a password after a short period of inactivity (10 minutes at most).
- Do not reply to mass or chain messages sent by e-mail.
- Turn off equipment via the software, not by switching off the power button, to correctly end a session, except when the machine blocks.
- Log off systems at the end of your work day.
- Do not leave accessible IT materials such as diskettes, cassettes, CD-ROMs, etc., containing confidential data, unsecured.
- Do not forget to collect sensitive documents received, sent, printed or photocopied, from fax machines, printers and photocopiers.
- Do not install any equipment, software or programs on networks and information systems without obtaining the prior authorization and assistance of all relevant departments in the company or Group.
- Take all necessary physical measures to protect equipment against theft, especially by locking cupboards, filing cabinets and offices, even when away for a short time.
- Should any equipment be stolen, notify the local IT Security Officer or Helpdesk immediately.
- **Persons responsible for application development**, should test applications that are developed in-house or sourced outside in the correct development, test and production environments and in the proper order.

Action may be taken against persons who do not comply with the guidelines above, if the breaches observed have harmed or are liable to harm the company and/or the Saint-Gobain Group, or their employees, or have been repeated despite warnings given.

---

1 Additional measures are to be found in the General Security Doctrine
3. Preservation of equipment, programs, software, etc., made available to users

For the performance of their professional tasks, the company makes available to users computer resources and communication networks which comply with applicable legal and technical regulations and with standards set by the company. Consequently, users are prohibited from modifying these standards, particularly by adding non-standard software for which the company could, in addition to potential problems of incompatibility, be charged with piracy.

Hard disks at workstations, as well as network disks, must not contain any programs, software, documents, files, information or data, which are pornographic in character, or liable to incite hatred, violence or racism, together with any other files forbidden by law.

Users of portable equipment agree to take the necessary security measures with respect to their equipment and access to the data it contains, wherever they may be. They must never transport a complete set of files which might be of strategic value for the company and/or the Saint-Gobain Group.

The computer resources made available to all users, and specifically hard disks, may be checked and controlled by the company (see Appendix 1), within the scope and terms of the law.

4. Protection against computer viruses

All users’ workstation, file servers and electronic mail systems are in general equipped with antivirus software. However, using communication applications such as internet and electronic mail systems, and storage materials such as diskettes and CD-ROMs, may, despite precautions taken, lead to programs or files which corrupt or steal data and software being sent to and installed on users’ workstations, without their knowledge.

Should there be any anomalies, users should stop all operations and immediately warn the relevant IT Security Officer or Helpdesk.

5. Using electronic mail systems

As everywhere else, proper behavior is a fundamental principle in all electronic exchanges.

Users should never write anything in electronic messages that they would refrain from expressing orally or by other means such as by post or fax, since electronic messages can:

- Be stored, re-used, and exploited for purposes that users had not considered when writing them.
- Constitute evidence or prima facie written evidence.

In addition, users should write short, clear messages to avoid information overload detrimental to effective communication. They should also use personal and group distribution lists with discretion. They should avoid putting an unnecessary number of addressees in copy.

Lastly, users are reminded that electronic messages sent from one entity to another within the Saint-Gobain Group are generally regarded as secure.

In most other situations, electronic messages flow through the web and can therefore at any time be intercepted, displayed, recorded, modified and used for other purposes by a third party, particularly industrial espionage, which requires that users take all precautions to avoid these risks.
6. **Using internet**

Internet is a tool placed at the disposal of users for professional purposes. Users should therefore use it appropriately.

This access enables users, as needed, to visit sites worldwide, using the company name. Indeed, when users browse the web, their identifier is shown as “Saint-Gobain” on external sites.

Everything users do, as well data relating to them – sites visited, messages exchanged, data supplied in forms, data collected without users’ knowledge, etc. - can be recorded by third parties, analyzed to find out their centers of interest, company projects, etc. and used for commercial or other purposes.

Consequently, users should take all necessary precautions in this regard.

For statistical, quality and security purposes, internet traffic is regularly supervised, checked and audited by the company, within the scope and terms of the law. *(See Appendix 2)*

7. **Using discussion forums**

Discussion forums should adopt the same rules of precaution and good practice as electronic mail systems.

They are a major source of industrial espionage.

Users’ sense of responsibility should restrain them either from disseminating any information likely to harm the industrial and/or commercial interests or corporate image of the company and/or the Saint-Gobain Group, or even from participating anonymously in these discussions.

8. **Responsibility with regard to information, data and files**

The company is responsible for:

- Supplying secure computer resources and communication networks in compliance with applicable legal and technical regulations, and with the standards set by the company with regard to their everyday use.

- The technical maintenance of computer resources and communication networks and their operation within secure conditions of everyday use.

Users, whatever their position in the company, should ensure that their files, data, information, etc. remain lastingly available, enabling other persons or users to have read only or full access to them when required.
9. **Duty to be vigilant**

All users are required to notify their IT Security or Helpdesk of any attempted violation of their workstation, files or data, or electronic mail system, as soon as they become aware of it.

**PROTECTION OF CONFIDENTIAL DATA**

Users should avoid the risk of divulging any confidential data to be sent, received or processed, for professional purposes, via the communication network: files containing information on personnel matters, financial results, draft contracts; order books, strategic industrial and/or commercial projects, research programs, market studies or studies of new products, business secrets, manufacturing secrets, etc.

Given the insecure nature of internet, users should not use it for sending or having sent to them any confidential information without taking the necessary safety precautions, such as passwords or encryption, to prevent its being disclosed. The same applies when users wish to send confidential information by electronic mail.

**COMPLYING WITH LEGISLATION PERTAINING TO THE PROTECTION OF INTELLECTUAL PROPERTY**

With the assistance of the Legal Department, users should obtain all necessary prior authorizations if they wish to reproduce or send via the communication network, including intranet, any newspaper articles, extracts from books, photographs, brand names or logos, drawings or designs (shapes of objects, etc). All information sent, received, or stored on a workstation or company server remains the property of the company.

Users should not load, store or send files containing material protected by legislation pertaining to intellectual property, unless they have been given the necessary authorization. They shall refrain from asking third parties to send them enclosures of such files.

Similarly, users agree not to use the equipment, programs, software, software packages, etc. which the company has made available to them, in a way that would infringe laws relating to intellectual property, relevant technical regulations and company standards.

**COMPLYING WITH THE MANDATORY DECLARATIONS TO THE FRENCH NATIONAL COMMISSION FOR INFORMATION TECHNOLOGY AND CIVIL LIBERTIES (CNIL)**

If users are required to set up or modify systems dealing with the processing of personal data; i.e. personal files or data banks, they should first contact the Legal Department in order to make a declaration to CNIL.
THE DUTY TO BEHAVE SUITABLY WITH CORRESPONDENTS AND THE OBLIGATION OF LOYALTY OWED TO THE COMPANY AND THE SAINT-GOBAIN GROUP

When users use communication networks they can be made liable, together with the company, for the remarks they make or terms they use.

They should therefore at all times behave properly towards their correspondents and show discretion and loyalty to the company and the Saint-Gobain Group.

Specifically, users should:

- Not express personal opinions outside the scope of their professional activity
- Refrain from expressing any remarks liable to damage the company or companies in the Saint-Gobain Group, their managers and/or employees, as well as any other corporate body or individual whatever
- Avoid engaging their responsibility or that of the company or others, through the circulation or reproduction of any information which is false; malicious, discriminatory or liable to prejudice the honor and/or probity of others.

COMPLYING WITH THE CHARTER

All users of computer resources and communication networks, which the company has made available to them, shall agree to comply with this Charter.

Control audits shall be carried out within the scope and terms of the law.

The company undertakes to set in place, within existing technical constraints, all appropriate means to achieve the best possible security for facilities made available to users.

PUBLICISING THE CHARTER

This Charter is the result of an information/consultation process conducted with staff representatives and has been drawn to the attention of all company employees.
APPENDIX 1 – INSPECTING THE OPERATION AND INTEGRITY OF SYSTEMS

Individual computers and servers are inspected on a regular basis or when required by incidents, etc., with regard to the operation and integrity of the system, as well as the content of hard disks and network disks, as follows:

- Searches for malicious software, such as viruses, worms, Trojan horses, spy software, etc.
- Inspection of standard company settings, especially security
- Software inventories to check the outcome of maintenance work, check licenses, identify prohibited and/or dangerous software
- Equipment inventories
- Identification of unused accounts
- Analysis of journaling files and/or temporary directories. In fact, all operating systems software and most applications and database software offer internal journaling capability. These journals make it possible to identify, analyze, and if necessary, reproduce an incident. They have been declared to CNIL (French Authority for Personal Data protection) like all operating systems and applications software that handle personal data.

APPENDIX 2 – SECURITY OF INTERNET CONNECTIONS

1. The general rules as stated in section 1 of using computer resources apply to all Web site access.
2. The reporting of disclosure requests of the French CNIL apply only to French Web sites.

The Saint-Gobain Group’s internet connections are or will be managed on a shared basis by Saint-Gobain Telecom.