IT Charter

(Charter for the use of communication tools & IT resources)

Preamble

The company provides its employees with IT resources and electronic or digital communication tools, namely the computer, the telephone, the Intranet, the Internet and electronic messaging (hereinafter the "IT Resources").) as well as information and data (databases, images, video, etc.) which are necessary for the performance of their functions.

The use of these resources is likely to create risks, of which the employee is not necessarily aware. It is therefore appropriate to inform everyone about these risks, the need for responsible use, the practical arrangements for this, and the existence, for safety purposes and risk management purposes, of civil or criminal liability of the company, monitoring and control means that it can use.

CHAPTER 1. GENERAL

1.1 PURPOSE OF THE CHARTER - SCOPE OF APPLICATION

The purpose of this Charter is to set out the main rules and precautions that all users must respect and implement when using IT Resources.

It concerns all users of IT Resources.

All employees of the company, including those working outside the company, as well as, to the extent that they have access to IT Resources, interns and workers made available to the company are considered "users". by temporary employment companies or by third parties as well as employees of external companies involved.

This Charter is distributed to all staff concerned.

1.2 COMMITMENTS

Each user undertakes to know and apply all the provisions of this Charter.

The company undertakes, for its part, to implement relevant and proportionate means, taking into account the state of technology and needs, in order to guarantee the security of the installations and IT Resources made available to users.

1.3 FUNDAMENTAL PRINCIPLES

The user is responsible for the use he makes of the company's IT Resources in the exercise of his function.

He must reserve the use of these Resources within the framework of his professional activity.

Furthermore, when consulting, creating, disseminating, making content and/or messages available via Computer Resources, each user undertakes to comply with the applicable legal and regulatory provisions.

As such, the user is prohibited in particular from using the company's IT Resources for:

- Upload, store, distribute, access or be sent documents, information, images, videos, content or messages of any nature or form:
  - o of a violent, pornographic, pedophile or contrary to good morals nature;
  - o likely to undermine respect for the human person and their dignity, as well as the protection of minors;
  - o of a defamatory, illicit, insulting, outrageous, misleading or slanderous nature towards third parties, natural or legal persons;
  - o likely to undermine the integrity and conservation of company data and their processing;
  - o likely to harm the internal and external brand image of the company;
  - o likely to constitute an apology for crimes against humanity or war crimes, an apology for Nazism, an apology for crimes or offenses, challenges to the existence of crimes against humanity or recognized genocides; constituting an act of counterfeiting, unfair competition or parasitism

o of a racist, xenophobic, negationist nature or damaging to the honor or reputation of others, inciting discrimination, hatred or violence against a person or group of people because of their origin, their sex, their family situation, their physical appearance, their surname, their state of health, their disability, their genetic characteristics, their morals, their true sexual orientation or supposed, of their age, their political opinions, their trade union activities, their true or supposed belonging to a specific ethnic group, nation, race or religion;
o infringing on private life, the intimacy of private life, or the image rights of individuals
o inciting to commit an offense, a crime or an act of terrorism.

If the user receives, without his knowledge, elements having one or other of these characteristics, he is required to destroy them.

- Use the company's IT Resources for the purposes of harassment, threats or insults and generally to violate existing rights.
- Load, store, transmit or be sent programs, software, software packages, etc. or files containing elements protected by intellectual property laws, unless you have the necessary authorizations.
- Use the materials, programs, software, software packages, etc., made available by the company, in violation of intellectual property laws, applicable technical rules and requirements defined by the company.
- Knowingly upload or transmit files that contain viruses or corrupted data, worms, Trojan horses or any other computer programs that may interrupt, destroy or limit the functionality of any closely or closely related computer or computer network. away from the company's activities.
- Send or transmit chain messages (messages received individually as part of a collective broadcast with invitation to also send it back collectively)
- Participate in gambling games and discussion forums unrelated to the professional activity of the employee concerned,
- Use the company's IT Resources in such a way as to hinder the access of other users.
- Use the Resources in violation of the secrecy of correspondence, business secrecy, confidentiality of data or information.

As a reminder, some of the activities set out above may constitute criminal offenses.

1.4 USE CONTROL AND SANCTIONS

Users are informed that the company may carry out checks to ensure the proper use of IT Resources, whether upon internal request from authorized bodies or upon legal requests.
All users are responsible for their use of the IT Resources they access.
Failure to comply with the rules and security measures contained in this Charter entails the personal liability of the user; it exposes him to a restriction or withdrawal of his possibilities of access to IT Resources or, if necessary, to a disciplinary sanction.
The company reserves the right to prohibit the user from access, temporary or permanent, to electronic messaging, as well as access to navigation software allowing the consultation of illicit or prohibited sites, or to block any moment and without prior warning access to sites whose consultation is contrary to the provisions of this Charter.

IT Charter

(Charter for the use of communication tools & IT resources)

CHAPTER II. - USER GUIDELINES – SAFETY

2.1 SECURITY OF INDIVIDUAL POSTS

It is up to the user to contribute, at their level, to the security of the company's IT Resources.
In order to contribute to the general security of Computer Resources, including the network, the user undertakes in particular to respect the following rules.

- Always use a secure password (minimum of 12 characters including at least one capital letter, a number and a special character) to access your computer and your email;
- The password does not expire/anymore according to the latest ANSII recommendations, but you must use a different password for each access;
- never lend it or communicate it to other users, even to the network administrator, or to third parties; the password being personal and confidential;
- specifically protect confidential files by using confidentiality labels;
- use the network's antivirus on any document from outside the company;
- do not respond to mass or chain messaging messages;
- turn off your workstation by software shutdown and not by switch (except in cases of technical blockage) at the end of each work period;
- never leave your workstation without locking it, thus leaving resources or services accessible to everyone (putting it on standby with a password after five minutes of inactivity is only additional protection);
- not leave computer media (USB key, external HDD hard drive, SSD drive, etc.) containing confidential data available to others in an open office;
- do not forget to retrieve confidential documents from faxes, printers or photocopiers;
- do not use an auto-start USB key (example of type U3) from a person external to the company on their workstation;
- protect the reading of all confidential documents on USB key;
- ensure the protection of its information by using the various backup means made available to it, whether individual or on networks;
- report to the person responsible any attempted violation of his account, any theft of his identity, and in general, any anomaly he may notice
- undertake not to allow access to IT Resources to any unauthorized person;
- not use another user's navigation software and communicate their access code to this software;
- not download, display, transmit by email or in any other way, open any file (image, sound, text), which would be prohibited by law
- not participate in unprofessional online conversations (“chat”);
- Do not participate in non-professional forums
- do not download software, whether free or not, without the prior agreement of the IT department on workstations connected to the company network.

2.2 HARDWARE, PROGRAMS, SOFTWARE, ETC.

To carry out its professional activity, the company provides the user with tools (computer, telephones, fax, etc.) that comply with the applicable legal and technical rules and the rules defined by the company. The user is therefore prohibited from modifying these rules, in particular by adding software not specifically authorized, in particular for which the company could be accused of piracy, apart from potential incompatibilities. As a precaution, certain configurations may be locked by the company (workstation, etc.)

The hard drive of the user's workstation must not contain programs, software, documents, files, information or data, as recalled above, in particular files of a pornographic, Nazi or racist nature as well as any other file prohibited by law. The “Desktop”, “Documents” and “Pictures” folders are synchronized with Microsoft Onedrive for each user and for use at their discretion to facilitate file backups. The user is responsible for saving their data in these directories.

Laptop users are committed to securing their hardware and access to the data it contains, wherever they are. The user should never transport entire files that would have strategic value for the company. Systematic use of an anti-theft cable, when available. In the absence of an anti-theft cable, never leave the laptop exposed on the desk when you go for lunch or in the evening; store it in a locked cupboard or desk.

Although public Wi-Fi offers invaluable convenience, it is essential to take security measures to protect your personal and business data. By adopting these few best practices and remaining vigilant, you can minimize risks and enjoy a more secure connection.

• Favor your 3G/4G/5G connection sharing instead of public Wi-Fi whenever possible

• Use a Virtual Private Network (VPN)

• Turn off file sharing if you "need" to connect to public Wi-Fi networks

• Avoid sensitive transactions (such as banking transactions or online purchases, etc.)

• Do not connect to unknown Wi-Fi

• Enable firewall security settings

• Update your Software regularly

The means made available to any user, and in particular hard drives, may be subject to verifications and controls by the company, within the limits provided for by law.

In accordance with local legal provisions, for instance in France, the National Commission for Information Technology and Liberties as well as employee representatives are informed of the methods of controlling and storing the information collected.

2.3 COMPUTER VIRUSES

The workstation (station, microphones, laptop, etc.) of each user is generally equipped with antivirus software.

However, the use of communicating applications (Internet, messaging, etc.) and storage media (USB key, external HDD hard drive, SSD drive, etc.) may, despite the precautions taken, cause transmission and installation on Howa-Tramico Europe

The user's workstation, without the latter's knowledge, of programs or files, which alter or pillage the data and software it contains.

In the event of an anomaly, the user must stop all use and immediately notify the IT department.

2.4 ELECTRONIC MESSAGING

The use of electronic messaging tools is reserved for professional use.

Consequently, each user undertakes to only communicate their email address as a working tool.

Occasional use for personal purposes may be tolerated in exceptional circumstances but must not, in any case, have a negative effect on the user's salaried activity or harm the proper functioning of the IT resources. The user must then indicate, in the subject of the message, that it is of a personal nature and check the "private" distribution criterion.

The user must never write an electronic message that he or she would not express orally or by another means (mail, fax, etc.), because the electronic message can:

o be stored, reused, exploited for purposes which the user would not have thought of when writing it,

o Constitute proof or the beginning of proof in writing.

As everywhere else, courtesy is a basic rule in electronic exchanges.

In order to maintain effective communications, the user must ensure that messages are short and clear, and only distributed to the appropriate recipients, being particularly careful when using pre-established mailing lists.

Please note that electronic messages not internal to a site pass through the Internet and can therefore, at any time, be intercepted, viewed, recorded and used for other purposes by a third party without the knowledge of the company or of the user.

Messages sent externally must contain, at the signature level, information relating to the non-disclosure of the content.

Each user is invited to protect themselves against possible absences (absence message) in particular by sending multiple-use messages and documents to all interested parties,

For statistical, quality of service and security purposes, Internet email traffic is subject to regular supervision and audits by the Company, within legal limits.

The user acknowledges being informed that all emails sent or received in a professional capacity will be archived by a third party service provider of the company for the purposes of meeting the administrative needs of the company and for a period of seven (7) years.

2.5 INTERNET

The Internet is a tool which is made individually available to certain users in order to allow them to access Internet sites for professional purposes,

Only sites which have a direct link with the employee's activity may be consulted as long as the consultation is of certain usefulness with regard to their functions.

The discernment of each user is called upon so that the use of the Internet corresponds to the objectives of speed and efficiency linked to the implementation of this tool and complies with the legislation in force.

Generally speaking, the use of this tool must be fair, consistent with professional objectives, non-profit, non-gaming and limited in duration.

The user is informed that access to certain illicit or prohibited websites may be refused by the implementation of specific measures by the company.

The user is informed that the personal data which may be collected as part of the control of internet use by the company will be kept for a period of six (6) months.

Each website may be governed by legal rules other than French or local law, all precautions must be taken in this regard by the user; he must be aware that all his activity and traffic can be recorded by third parties without his knowledge and without the knowledge of the company.

2.6 TELEPHONY

The telephone system is made available to users to enable them to carry out their professional telephone communications, whether external or internal communications, within the framework of their professional activity,

The use of the telephone is thus reserved, except in exceptional circumstances, for professional use.

For all purposes, the user is informed that the company may be required to monitor the uses made of the telephone and that in the event of misuse of the telephone for private purposes, the company may demand reimbursement of the amounts corresponding to the abusive use to the user and take disciplinary sanctions.

Use of mobile phones for private purposes during working hours should be limited to emergency cases. It is strictly prohibited for employees working on automated machines or driving devices.

When traveling in unsecured spaces, it is not recommended to leave the Wi-Fi function of your smartphone permanently activated, as this could result in automatic connection to unsecured networks without your consent.

2.7 PROTECTION OF PERSONAL DATA

The applicable rules relating to the protection by the company Howa-Tramico and by users of personal data are described in the GDPR charter of the Howa-Tramico Group. The user can contact the Human Resources Director who has been designated Data Protection Officer (DPO) within the Howa-Tramico company for any questions about these practices.

2.8 CONFIDENTIALITY

As part of access to IT Resources, the user may have access to information, owned by the company, or made available to it, which cannot be disclosed to any third party whatsoever. This information may in certain cases be covered by professional secrecy or business secrecy and its disclosure is likely to cause considerable harm to the company.

In order to respect the confidentiality of Howa-Tramico company information, the user undertakes, during the duration hereof, to:

- o Use this information only in relation to and within the framework of the use of IT resources and its activity;
- o Keep this information confidential and not, at any time, divulge, disclose or communicate it to any third party;
- o In the event that the user wishes to disclose certain information published on the Computer Resources, to request the prior written consent of the DPO for this disclosure, specifying the purposes of the disclosure, the persons concerned and the measures taken. to ensure compliance with confidentiality obligations by third parties to whom this information has been disclosed.

These confidentiality obligations do not apply to information which was already in the public domain prior to the entry into force of this charter or is revealed to any user on a non-confidential basis by a source not contractually or legally bound not to not disclose such information

Howa-Tramico's service providers are also contractually bound by these confidentiality obligations, particularly when they are authorized to work on the company's equipment for the purposes of third-party maintenance.

CHAPTER III. - PUBLISHING

ARTICLE 3.1 - OPINION OF STAFF REPRESENTATIVES

This charter has been submitted to the Health, Safety and Working Conditions Committee for matters falling within their competence and for the opinion of the Central Works Council.

ARTICLE 3.2 - COMMUNICATION TO THE LABOR INSPECTION

This charter has been communicated to the Labor Inspectorate responsible for the Brionne establishment (factory and head office), accompanied by the opinion of the Health, Safety and Working Conditions Committee of the Brionne establishment. for matters falling within its jurisdiction.

ARTICLE 3.3 - ADVERTISING

This charter has been filed with the secretariat of the Industrial Tribunal for the location of the Brionne establishment (factory and head office).
It is also displayed in the Brionne establishment (headquarters and factory).

CHAPTER IV. ENTRY INTO FORCE

This Charter is immediately applicable upon distribution (which may be done by any means) to all users, one month after the filing and advertising formalities.
It is given by the company to any new user of IT or digital or electronic communication tools

Established at Brionne, the 25th of June 2018
Updated the 13th of December 2024

Howa-Tramico General Manager