IT charter: how to use it

Today, most employers provide their employees with IT resources to allow them to accomplish the missions entrusted to them. A "*charter for the proper use of new information and communication technologies*", commonly known as the "*IT charter*", which all employees must follow proves to be indispensable to control the access to these IT resources (workstations, shared network, Internet...) as well as to protect the data that pass through them, are stored, and exchanged.

This document written for the attention of the users comprises a set of rules that establishes the responsibilities of the different players and reconcile on one hand the employer's interests (to protect the entity's entire information systems) with, on the other hand, those of the employees (to guarantee their rights as well as their individual and collective freedoms).

The establishment of an IT charter helps to avoid all kinds of misuse of the IT tools and establishes a frame of reference in case of conflict assuming the charter is correctly deployed.

Finally, although this IT charter is not mandatory, it can be used as a means to inform users of the collection of their personal data for the needs of the information systems (IS) and the implementation of IT tools.

A code of good conduct

Intended to be used as a reminder of the rights and obligations of both the employees and the employers, the IT charter is now an essential element of the global information system security policy. By establishing a framework of standards and good practices for an optimal use of IT resources, it informs users in particular about :

- at-risk behaviours likely to damage the common interests of the company or the administration, as well as the requirements in terms of security;
- possible surveillance measures (phone tapping, video surveillance, and so on) implemented by employers in the work place;
- a framework defining the proper use of software tools and the limits between professional and personal use;
- the penalties applied in case of failure to apply the IT charter.

Its objective is to establish a policy consistent with the technical reality and human resources policies to address all of the risks.

Moreover, it must be deployed as an appendix to the work contract or to the company's rules and regulations.

The contents of the IT charter

The IT charter cannot be a standard document. Indeed, it must always be written to take into account the specific activity of the company or administration implementing it including specific security constraints. Its writing requires careful consideration often involving multiple services and/or departments, and it must obey to the principle of proportionality depending on the pursued purpose, which may require frequent updates.

The IT charter must indicate in particular the following themes:

Access management of the entity network and Internet

This section defines the rules relating to the identifiers and passwords communicated to employees to allow them to connect to the company network and to the Internet.

The credentials (identifier and password) of the user are strictly personal, it is therefore necessary to forbid their disclosure to another employee or third party with the exception of the situations described in section "*Leave management*" herein.

It is also recommended to ask users to lock their sessions (screensaver with password) when they leave their workstations and to plan measures to block accounts after a certain number of failed attempts to connect.

Furthermore, access rights to particular files or folders could be restricted to authorised users only. This clearance policy must be defined taking into account the respective responsibilities of each user and, where applicable, the sensitive nature of the data being processed.

The conditions of use of the professional messaging system

It might be indicated in this section that a limited and reasonable use of the professional messaging system for private purposes is tolerated.

The respect of the confidentiality of private correspondence is an inviolable principle, the employer shall therefore not access the content of private messages sent from or received by his or her employees on the professional messaging system without the presence of the said employee.

However, for such messages to be considered private, employees must identify them as such, for example:

- by indicating in the subject line of the message words such as "*private*", "[*PRV*]", or even "*personal*";
- by mentioning in the subject line of the message an indication that denotes the obvious private nature of the message, such as, "*holidays in Japan*";
- by storing such messages in a folder entitled "*personal*" or "*private*".

Furthermore, employees must also be reminded that messaging shall not be used to commit any violation of the law, whether by the contents conveyed or by the words that were exchanged. Under no circumstances shall messages include contents susceptible to endanger the security of the information system (for example, oversized or at-risk attachments). Anti-spam and antivirus systems may therefore place certain messages in quarantine.

It is also necessary to indicate if the log files from the messaging system are susceptible to be verified for security purposes of the IS and maintenance and/or to detect any misuse of the messaging system with regards to the established rules (for example, too many messages flagged as personal, problematic volume or nature of the attachments).

The conditions of use of the Internet

It may be reminded in this section that the internet connection made at the disposal by the employer shall be used for business purposes, but private use may be tolerated as long as this use remains reasonable. This criterion of reasonableness might be, for example, a specific time slot (or duration) of the connection after which the use of Internet for private purposes shall be considered excessive.

Furthermore, it should be reminded that an employee is expected to refrain from committing any act that might be in violation of the law, or that might jeopardise the security of the information system in any way whatsoever, through inappropriate use of the Internet (downloads, consulting at-risk sites, and so on).

The employer might also decide to prohibit access to certain sites (pornographic, discriminatory, violent, or more broadly, contrary to public order and to good moral standards, social networks, and so on).

Furthermore, when the log files reflecting the overall use of Internet within the company or administration are checked for IS security and maintenance purposes, it shall be mentioned in this section.

The conditions of telephone use

This section should specify whether private phone calls are tolerated and whether a control is carried out.

When a device to record phone conversations is installed, it is necessary to describe precisely, notably, the detailed steps of the control, its terms and conditions, the telephone devices impacted (fixed or cell), the final purpose of the intended controls, and the conditions of the right of access.

Furthermore, the APDP recommends that the charter include the possibility to deactivate the recording function by pressing a predefined key on the telephone before making a private call, assuming that the company tolerates that the telephone be used for private purposes. Otherwise, if this is not the case, it will be necessary to authorise the collaborator to use a telephone on his or her work place that is not subject to being recorded, or to use his or her personal cell phone.

Leave management

The charter must provide a procedure to access the electronic mailbox by authorised persons in case of a temporary absence or permanent leave of a user. In this respect, the charter must indicate that it is possible to access the electronic mailbox of the absent person only for reasons strictly necessary to ensure the continuity of the activities of the company and administration, provided that the emergency of the situation justifies it.

For example, the charter may provide a way to set up an automatic out-of-office reply to the sender of the message to indicate a person to contact in case of an emergency, appoint a substitute who has the same access rights to the mailbox of his or her colleague, or even transfer all incoming messages to a substitute.

However, it must also specify that the substitute shall under no circumstances read any messages identified in the subject line as "*personal*", or "*private*", and that the employee must be informed of the identity of his or her substitute.

The same rules shall apply with regards to the access of the workstation of an employee who is absent.

Finally, in the event of the permanent departure from the company or administration, the employee's accounts and mailbox shall be deactivated within the three months following the departure of the said employee.

The obligation of confidentiality and security

It is important to restrict users to an obligation of confidentiality with regards to all the data to which they have access.

The employees shall for that matter demonstrate common sense and loyalty in how they manage the IT resources placed at their disposal.

The protection of personal data

The IT charter must imperatively inform users of all of the automated processing of personal information that have been implemented by the company or by the administration.

In accordance with Article 11 of Law no. 1.565 of December 3, 2024, this information must include the following information:

- **the identity and professional contact details of the data controller**, and, where applicable, its **representative** in Monaco;
- the **purposes** of the processing and **its legal basis**;
- **the legitimate interests pursued by the data controller or by a third party where the processing is carried out on such a basis;**
- the **categories of personal data** concerned;
- **how long the data will be retained** or, where this is not possible, the **criteria used** to determine this period;
- whether replies are **mandatory or voluntary**, and the consequences for the data subject in case of failure to reply;
- where the processing is based on the **data subject's consent,** the right to withdraw that consent at **any time**;
- the **recipients** or **categories** of recipients;
- the **means of exercising right of access, opposition, rectification, erasure, restriction or portability**;
- the **right to object to the use on behalf of third parties**, or the **communication** to third parties, of personal data **for prospection purposes**, in particular commercial prospection;
- the **right to lodge a complaint with the Personal Data Protection Authority (APDP)**;
- where applicable, the **contact details of the Data Protection Officer**;
- where applicable, the existence of an **automated decision-making**, including **profiling**, and **the reasoning** behind the processing;
- where applicable, the fact that the data controller carries out or intends to carry out a **data transfer outside the Principality**;
- the **source of the personal data** that are not collected directly from the data subject.

The penalties

It must be clearly specified when a failure to comply with the provisions of the charter is subject to a disciplinary or judiciary procedure in case of a violation of the law. These penalties might be mentioned, it being specified however that they cannot be contrary to the rules defined by labour law and shall comply with the principle of proportionality.

The IT administrator's charter

In parallel to the IT charter, which concerns all the users, the APDP also recommends the implementation of a specific charter for IT administrators. These latter have in fact particular rights and obligations, especially with regards to their access to data that can be private and to their obligation of confidentiality. Therefore, it is necessary to lay down the rules of professional conduct to which they are committed.

The IT administrator must in particular:

- not read any of the users' personal data, except, periodically, on the express request of the user him or herself, and must not grant access to anyone, except in particular cases provided for by law (for example, judicial enquiry) or upon previously declared formal and legitimate authorisations;
- comply to his or her obligations of confidentiality and non-disclosure by not reporting nor using the information that he or she may be given to learn within the scope of his or her activities;
- not connect to an IS resource without express authorisation from the person to whom the resource is allocated, in particular, in the case of using remote control software on a user's workstation;
- not take advantage of his or her privileges and to limit his or her actions to only those IT resources of which he or she has the responsibility, by respecting the final purpose of his or her mission (he or she must not modify any configurations and access rights other than in compliance with the predefined administrative or operating procedures);
- not take orders from an unidentified person and to inform his or her immediate supervisor of any request that he or she feels is inappropriate;
- not circumvent established security procedures, and in particular, not deactivate on his or her own initiative the tracing mechanisms, and not interfere with the integrity of the log files;
- log all of his or her actions.