

**COMPANY**

**Information security charter for IT administrators**

General information

Version: 0.8

State: Draft

Project: Information security charter for IT administrators

Date: 03/12/2018

Representatives:

# Object

The IT administrator is a key person who must have special privileges to perform his or her duties within the information system. As such, his professionalism and rigour are essential. The charter defines the code of conduct to the administrator in performing his or her duties.

# Definitions

The term "IT Administrator" refers to any person, whatever their function, whose role and missions are to ensure the proper functioning and security of information systems resources under their responsibility: such as servers, network equipment, security equipment, applications, databases, user workstations, etc.

In the rest of the document, the IT administrator will be referred to as the administrator.

# Code of conduct of the administrators

The administrator is subject to an obligation of confidentiality related to his activities, in this context:

* He does not abuse his status or the privileges associated with his position to gain access to information not directly intended for him or not necessary for the execution of his duties.
* He only gives access to information or a system to a third party in the course of their duties and/or at the explicit request of his superiors in the context of formalised procedures or in the specific cases provided for by law.
* He shall not abuse his status or the privileges associated with his position to gain access to users' personal data, except occasionally at the formal request of the user himself, and shall not authorise anyone to gain access to it, except in special cases provided for by law (for example, at the request of the public prosecutor in the context of a judicial inquiry) or formal and legitimate authorisation previously declared.
* He does not abuse his status or the privileges associated with his function to access content marked as "private" except in the presence and with the authorisation of the user.
* He respects the confidentiality commitments associated with his function or any specific related contract signed by him or his organisation. He shall not disclose or use confidential information that he may become aware of in the course of his duties, neither during his contract nor after its termination.
* He does not connect or instruct a third party to access an IS resource without the authorisation of the person to whom it is assigned, particularly in the case of the use of remote control software on a user workstation.

In addition:

* He documents his actions and interventions in such a way that the colleagues can continue interventions and maintenance in case of his absence.
* It is the responsibility of the employee to report security incidents or issues to his or her supervisor.
* He shall not take any initiative that could harm the interests of the company and shall act in good faith in all circumstances.

In addition, the administrator strictly observes the safety rules and limits his interventions:

* He does not abuse his privileges, and limits his actions to the IT resources for which he is responsible, while respecting the purpose of his mission. In particular, he shall only modify configurations and access rights in accordance with defined administrative or operating procedures.
* He does not take his instructions from an unidentified person and forwards to his superior any request he considers inappropriate.
* He does not bypass established security procedures, and, in particular, does neither disable traceability mechanisms on his own initiative nor compromise the integrity of log files.
* He only uses privileged accounts for activities and needs directly related to the administrative or operational tasks for which he is responsible, since any action on information systems can be logged to ensure their accountability.

In the event of an information security incident:

* He informs his superior and, as the case may require, the person in charge of the security of the information systems of his entity, of any security breach or incident that he may discover or of which he may become aware.
* It preserves, and saves the "traces" necessary for the resolution of an incident and any subsequent investigation.

Finally, the administrator ensures the protection of access rights related to his function:

* He complies with the security rules in place to protect the use of the accounts and privileges assigned to him.
* He ensures the protection of the workstations from which he performs his duties, the management of identifiers and authentication of privileged accounts.
* The authentication settings used for administrator operations must be robust and managed according to best practices. They are personal and non-transferable.

# Compliance with legislation and this charter

The IT administrator will comply in all circumstances with the current legislation, in addition to the rules of this charter.

In the event of non-compliance between the current legislation and the provisions of this charter, the IT administrator will be held responsible for his actions and may incur sanctions, as well as any other civil or criminal sanction provided by law.

This document is only a help in creating a security policy for IT administrators. It outlines some best practices and instructions to be followed by the administrators concerned. The information contained in this document is not exhaustive and should always be customised to the receiving organisation, knowing that a good practice can be accepted, adapted or even rejected depending on the context.

This charter does not in any way substitute the possible application of other charters to which the administrators must comply with.

Neither NC3, nor any of its representatives, can be held responsible for the use and consequences resulting from this text.

TO BE DELETED when putting the charter into context.