

**COMPANY**

**Information security charter**

General information

Version: 1.5

State: Draft

Project: Charter of information security

Date: DATE

Representatives: AUTHOR

# Word from the administration

Our organisation works with sensible information during our missions. To ensure the security of that information, I decided to put in place a charter of information security.

All of our collaborators are encouraged to read and apply good practices, described in this document.

This document is not meant to replace or negate existing documents.

<<ADMINISTRATION>>

# Material use for private business within the organisation

It is accepted to use the material at the employee's disposal for his private affairs, as long as the usage is reasonable and within reasonable limits. This type of usage should never trouble or disrupt any of the information systems and should not compromise the work of the employee himself or that of his colleagues.

# Usage of the information system

Following guidelines have to be respected:

* It is prohibited to use the organisation's resources to physically or morally harm a person's integrity or to damage the image of the organisation;
* The legislation currently in place is to be known and applied by everyone;
* Employees are not able to go beyond their given permissions and authorisations without prior authorisation: this means modify, reproduce, destroy or read information that is not destined for them;
* To collaborate with the maintaining personnel facilitating the identification and correction of emerging problems and anomalies.
* The material at the personnel's disposal will be used, manipulated and stored with care to avoid deterioration;

# Password management

Work related passwords have to:

* Be changed regularly (depending on the length of the password – common sense);
* Be at least 12 characters long
* Contain at least upper and lower case letters as well as numbers and punctuation/special characters.

The employee is personally responsible for the protection of his/her password. It is strictly prohibited for the employee to:

* Keep the default/given passwords after the first login, unless it is not possible to change it;
* Use simple to guess passwords (user name, pet name, birth date, telephone number, dictionary name, etc.);
* Use the same password throughout multiple systems;
* Give the password to anyone
* Send or distribute the password by email, telephone, Internet, etc;
* Write down the password without sufficiently protecting the written down password

Generic accounts, known by more than one person are proscribed.

An exception can be made for systems not accepting these types of restrictions (pin code of a smartphone for example)

# Usage of electronic material

Employees having a computer at their disposal engage themselves to:

* Protect access to their computer by password;
* Block access to the computer when leaving their workplace, even if the absence is very short
* Never leave their computer with third parties except if it is the maintenance personnel;
* Taking the necessary preparation to save every information locally stored (no backup).

The users know that personal information, possibly saved in the network, may be saved and kept as stated by current backup policies.

## Use of a Notebook, laptop or Smartphone

All the valid directives for computers are to be applied to notebooks, laptop and smartphones.

Additionally, the mobility of such devices requires particular attention of which the employee takes full responsibility.

All employees using this type of machine engage themselves to:

* Take all appropriate measures to ensure the physical security of these mobile devices at their disposal, especially preventing any theft or physical damage;
* Never to transmit confidential information through untrusted information networks;
* Saving the data stored on their mobile device;
* Taking precautions so that no other person can see the confidential information while using the mobile device in a public place.
* Every device containing sensitive information need to be encrypted.

# Usage of internet services (web)

The Internet is only to be used if the following rules are taken into account:

* If the user enters sensible information, he needs to be certain that he is on the requested site and not on a phishing site. The user needs to verify if he is really on a secured connection.

This can be done by looking for the appearance of a lock at the bottom of the browser or if the URL of the visited page starts with "https";

* It is prohibited for any user to navigate on pages containing insults, racism, paedophilia, blasphemous or violent content or any other damaging or illegal content.
* It is prohibited to download anything that is damaging to the information system or is not in compliance with legislation. When in doubt, it is best to abstain oneself.

# Usage of electronic mail

Email, just like any other type of mail is subject to certain rules:

* attachments are subject to good practice guidelines (taken into account the size of the attachment);
* If a user receives a message resembling spam or if the message is a hoax (means: containing unverified information), the user himself needs to think and verify that information before accepting and retransmitting the message. When in doubt, do not retransmit the content;
* the user is not to click on any link in the email's content if he did not verify that the email comes from a trusted source;
* The electronic mail is an insecure means of communication. Only public information should be sent in plain text, every other information has to be encrypted before transmission.

The following actions are prohibited:

* transmitting spam, chain mails or even joke mails are strictly prohibited, be it internally or externally
* transmission of content suppressed by the law of Luxembourg
* all inappropriate usage that could compromise the security of the electronic messaging system or could engender prejudice for the organisation is strictly prohibited

# Clean workspace

All papers or other removable information containing sensible data should never be unattended on the desk. Papers should be immediately taken from printers or copy and fax machines. Every workplace should be clean and organised if these are in publicly accessible or visible zones.

# Waste management

Before scrapping or reusing material in another context, it should be completely wiped. The procedure for this should be adapted to the sensitivity of the data previously stored on the material. Sensible documents will be shredded.

# Penalties

Intentional disregard, be it uniquely or repeatedly, of any of the rules in this charter, of the penal code, of the law for privacy or any disregard for intellectual property will result in disciplinary processes or legal consequences.