

(logo company)	Information security (title)	PO 01 (codification)
06/04/2021 (print date)	1/5 (page x of y)	001 (revision)

Information security

1. Subject
2. Purpose
3. Scope
4. Responsibility
5. Records
6. Requirements of ISO 27001: 2013
7. Information security policy
 - 7.1 Introduction
 - 7.2 Policies
 - 7.3 Criteria
 - 7.4 Principles
 - 7.5 Objectives

History

All	Creation	01/01/2021
Page	Change	Date

Auteur / fonction	Vérifié / fonction	Approuvé / fonction
/	/	/

(logo company)	Information security (title)	PO 01 (codification)
06/04/2021 (print date)	2/5 (page x of y)	001 (revision)

1. Subject

The subject matter of the information security policy is the strategy, organization and responsibilities for protecting information security against any internal, external, deliberate or accidental threat.

2. Purpose

The purpose of the information security policy is to ensure the continuity of the activity of the organization by reducing the risks and impacts of information security incidents.

3. Scope

The information security policy applies to:

- all staff
- all departments of our organization
- all digital and paper assets of our organization
- the work environment
- management tools
- the work with suppliers

Information security rules and measures concern physical access to premises, staff, technical resources and software.

4. Responsibility

The information security manager (ISM) has the authority to write and update the information security policy. He is responsible for its application and communication. The information security policy is validated by the director.

5. Records

Job descriptions

6. Requirements of ISO 27001: 2013

5.2 Policy

Top management shall establish an information security policy that:

- a) is appropriate to the purpose of the organization;
- b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
- c) includes a commitment to satisfy applicable requirements related to information security; and
- d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

- e) be available as documented information;
- f) be communicated within the organization; and
- g) be available to interested parties, as appropriate.

Auteur / fonction	Vérfié / fonction	Approuvé / fonction
/	/	/

(logo company)	Information security (title)	PO 01 (codification)
06/04/2021 (print date)	3/5 (page x of y)	001 (revision)

A.5.1.1 Policies for information security

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

7. Information security policy

7.1 Introduction

The information security management system (ISMS) is an essential lever for the performance of our organization. Ensuring information security is ensuring the survival and competitiveness of our organization.

Identifying sensitive assets and putting into practice protection, prevention, detection, assurance and remediation measures allows us to ensure the confidentiality, integrity and availability of our assets.

Sensitive assets, among others, are:

- staff with privileged authorities
- essential applications and systems
- application servers
- web servers
- database servers
- networks
- computers
- projects under development

The [Assess Risk](#) and [Treat Risk](#) processes help us define:

- what to protect
- from whom we must protect our assets
- how to protect our assets at all times

The responsibilities and authorities of personnel to establish, apply, monitor, maintain and improve information security are described in the [Job descriptions](#).

The direction:

- approves information security policies
- change, if necessary, policies during the management review
- identifies information security objectives
- support information security activities and initiatives
- provides the necessary resources to maintain the ISMS
- assigns responsibilities and information security authorities in the organization
- plans and implements information security awareness activities

7.2 Policies

This information security policy is supplemented by the policies:

Auteur / fonction	Vérfié / fonction	Approuvé / fonction
/	/	/

(logo company)	Information security (title)	PO 01 (codification)
06/04/2021 (print date)	4/5 (page x of y)	001 (revision)

- Mobile devices
- Teleworking
- Asset management
- Access control
- Cryptography
- Clean desk and locked screen
- Malware protection
- Backup
- Vulnerability management
- Network management
- Development
- Supplier relationships
- Compliance
- Personal data

The information security policy is supported by our processes, procedures and all records.

7.3 Criteria

The protection of information is characterized by the following essential criteria:

- confidentiality - information is available only to authorized persons and is protected from any unauthorized disclosure, access or use
- integrity - protection of the accuracy and completeness of information
- availability - the information is accessible and usable on demand by authorized persons in a timely manner and in the manner required
- authenticity - information is what it claims to be
- accountability - possibility of attributing responsibility for a fact to a person
- non-repudiation - the impossibility of denying participation in the processing of information
- reliability - degree of confidence that can be placed
- traceability - information necessary to identify the origin and the route

7.4 Principles

The information security principles that we adhere to are as follows:

- the information security management system (ISMS) complies with laws, regulations and agreements
- the ISMS is established, maintained, tested and continually improved according to:
 - management commitment
 - the requirements of ISO 27001
 - best practices
- information security risk management:
 - is aligned with the strategic objectives of our organization
 - determines the appropriate measures for each level of risk
 - is incorporated into business processes
- information security is everyone's responsibility and duty
- the assessment of the most critical risks is sufficiently detailed
- risk treatment is proportionate (in some cases multi-layered approaches are used)

Auteur / fonction	Vérfié / fonction	Approuvé / fonction
/	/	/

(logo company)	Information security (title)	PO 01 (codification)
06/04/2021 (print date)	5/5 (page x of y)	001 (revision)

- the least privilege (restricted access) concerns all staff
- the administrator account is never used to browse the Internet
- anonymous and generic accounts (trainee, contact, guest) are deleted
- segregation of duties is strictly enforced
- it is preferable to use open solutions and not proprietary choices
- the staff is:
 - trained and made aware of the information security policy
 - informed of possible disciplinary measures
- software should be configured so that security updates are installed automatically

7.5 Objectives

The objectives to be achieved by our information security management system are as follows:

- maintain the confidentiality of information
- maintain the integrity of information
- comply with operational information availability requirements
- securely handle sensitive information
- keep your systems and applications up-to-date
- provide a regular restoration point
- increase the awareness, knowledge and skills of all staff on:
 - commitment to support the information security policy
 - compliance with security recommendations and restrictions relating to:
 - authentication
 - passwords
 - the use of networks
 - the use of electronic mail
- report and investigate all security incidents
- test business continuity plans
- encourage the participation of all staff in improving the ISMS
- ensure the daily support of the ISM to maintain the ISMS and the obligation to report regularly on the performance of the ISMS to top management

Auteur / fonction	Vérfié / fonction	Approuvé / fonction
/	/	/