mobelite

DOC ID : ISMS/ISP
Date : 31/08/2026
Version : 1.1

POLITIQUE DE SÉCURITÉ DE L' INFORMATION

INFORMATION SECURITY POLICY

ISO/IEC 27001:2022 Information Security Management System (ISMS)

Purpose

The purpose of this Information Security Policy is to establish and maintain the information security objectives of Mobelite in accordance with ISO/IEC 27001:2022. This policy ensures the confidentiality, integrity, and availability of all information assets, mitigating risks from potential threats, vulnerabilities, and impacts related to the organization's information systems and digital services.

Information Security Objectives

In alignment with ISO/IEC 27001:2022, the primary objectives of this ISMS are to :

Confidentiality

Safeguard all sensitive and personal data from unauthorized access or disclosure.

Integrity

Ensure the accuracy, completeness, and authenticity of information and processing methods.

Availability

Ensure reliable access to critical information and services by authorized individuals when needed.

Compliance

Maintain full compliance with relevant legal, regulatory, and contractual obligations.

Risk Management

Continuously identify, assess, and treat information security risks to maintain an acceptable risk level across the organization.

Leadership Commitment

The leadership of Mobelite is fully committed to the establishment, implementation, and ongoing improvement of the ISMS. Management will ensure the allocation of necessary resources, support for information security initiatives, and the active involvement of all employees in protecting information. Leadership will regularly review the effectiveness of the ISMS and ensure its alignment with organizational objectives and the changing threat landscape.

Continuous Improvement

Regular internal audits

to evaluate the effectiveness of the ISMS and identify areas for improvement.

Management reviews

to assess the performance of the ISMS, address nonconformities, and ensure that the system remains aligned with the company's strategic objectives.

Security awareness training

to ensure that employees are equipped to identify and mitigate security risks and are kept up to date with evolving threats.

Communication and Awareness

Clear communication is critical to the success of the ISMS. The following mechanisms will be employed :

Employee Awareness

Regular training sessions and communication to ensure that all employees understand their role in maintaining information security.

Customer and Third-Party Communication

Transparent communication about the company's information security practices to customers, partners, and third-party vendors.

Incident Notification

Procedures for notifying stakeholders promptly in the event of a security incident that affects their information or services.

Policy Review - This ISMS policy will be reviewed annually or more frequently, if necessary, in response to changes in the business environment, technology, regulations, or other significant factors. The policy may be updated or revised as needed to ensure its continued effectiveness.