



Information System Security Policy

Management Policy Statement · Aligned with ISO/IEC 27001:2022

Doc ID: PO-ISMS-17 | Date: 20-08-2026 | Version: 02

■ Policy Statement

Recognizing the inherent risks and opportunities of a growing digital landscape, Lanterns' General Management has established an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001:2022.

Lanterns continually reflects on how it protects the information and solutions it makes available to its users. Aware of these challenges and the associated risks, Lanterns has developed this information security policy, in consultation with all interested parties, to set the framework for information security.

Implementing this policy strengthens confidence and maintains a high level of satisfaction among our stakeholders. It reflects the importance Lanterns attach to protecting information, and enables Lanterns to accomplish its mission, preserve its reputation, protect its customers' data, comply with applicable laws, and reduce risk across the information it creates, receives, or holds. The policy follows a continuous improvement approach built on the ISMS, which enables the assessment, control, and management of information security risks.

■ Our Objectives

This policy aims to ensure:

Confidentiality	Information is not made available or disclosed to unauthorized people, entities, or processes.
Integrity	The accuracy and completeness of information assets is protected.
Availability	Information can be used on demand by an authorized entity.
Traceability	The system records the operations that are carried out.
Compliance	Applicable legal and regulatory requirements are met.

These objectives are translated into performance indicators (KPIs), deployed against identified processes, and calculated and analyzed periodically to drive continuous improvement.

■ Our Commitment

Given these objectives and the paramount importance of certification, General Management informs all staff of its firm and irrevocable commitment to:

- Operate and fulfill the information security management system;
- Provide the resources and means necessary for its achievement and improvement — training, time, and investment;
- Meet all applicable requirements: legal, regulatory, internal, customer, and information security.

APPOINTMENT

The Chief Information Security Officer (CISO), with the authority to establish, monitor, maintain, and improve the ISMS.

We urge all staff to fully embrace this system and to make every effort to design, implement, and continually improve it.

Chief Information Security Officer

Chief Executive Officer

Jihed Jaouabi