Lanterns STUDIOS	**Information System Security Policy – One page** **« Lanterns »**	Doc ID: PO-ISMS-17 Date: 22-09-2025 Version: 01

Information System Security Policy

Policy statement

Recognizing the growing digital landscape's inherent risks and opportunities, Lanterns' general management has taken the proactive step of establishing an Information Security Management System (ISMS) in accordance with the rigorous international standards of ISO 27001:2022.

To address these risks, an organization that provides IT services should reflect on how it protects the IT information and solutions it makes available to users.

Aware of these challenges and faced with these risks, Lanterns develops an information system security policy, in consultation with all interested parties, to set the framework for information security.

The implementation of the said policy will make it possible to strengthen confidence and maintain a high level of satisfaction among its stakeholders. This information security policy reflects the importance that Lanterns attaches to the protection of information. It also allows Lanterns to accomplish its mission, preserve its reputation, protect its customers' data, comply with laws, and reduce risks by protecting the information it has created or received and of which it is the holder.

It follows a continuous improvement approach based on an information security management system. Enabling the assessment, control and management of information security risks, an information security management system is put in place.

Our objectives

The information security policy does not limit itself but aims to ensure:

- **Confidentiality of information**: information is not made available or disclosed to unauthorized people, entities, or processes.
- **Information integrity**: protecting the accuracy and completeness of assets.
- **Availability of information**: the information can be used on demand by an authorized entity.
- **Traceability**: the ability of the system to record the operations that are carried out.
- **Compliance with legal and regulatory requirements**

The objectives mentioned above are translated into performance indicators (KPIs). They are deployed against identified processes and are calculated and analyzed periodically for continuous improvement.

Given the objectives set on the one hand and the paramount importance of certification on the other, we inform all staff of the firm and irrevocable commitment to:

- Fulfill the information security management system.
- Provide the necessary and indispensable resources and intangible means for its achievement and improvement (training, time, and necessary investments).
- Meet applicable requirements (legal, regulatory, internal, customer, information security…)

As such, the Chief Information Security Officer (CISO) has the necessary authority to establish, monitor, maintain and improve the information security management system (ISMS).

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

CEO

Jihed JAOUABI