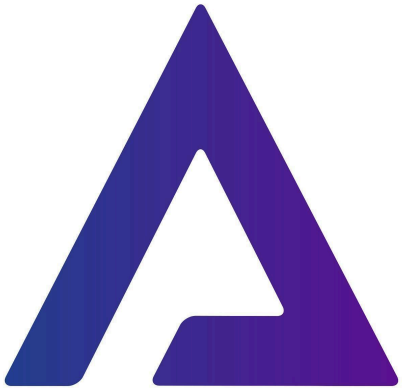

ADHARA

Integrated Information Security (WEB)

MS. 02.01

INFORMATION ABOUT THIS EDITION

	Prepared	Approved
Title	Head of IT & Security (Acting ISMS Manager)	ISMS Committee

Version	Date	Summary of changes / Comments
1.0	2026.3.20	Initial version

Adhara has chosen to manage its information systems and business continuity in accordance with international best practices and ISO 27001. Recognizing the critical importance of the information and services it provides, Adhara establishes, under the company's leadership, the following fundamental principles of information security and business continuity:

Principle of Regulatory Compliance

- All information systems and business processes shall comply with applicable legal, regulatory, and industry standards that impact information security and service continuity. This includes, in particular, provisions related to the protection of personal data, system security, data security, communications security, and electronic services.

Risk Management and Continuity Principle

- The aim is to minimize risks to acceptable levels, maintaining a balance between security controls, the criticality of information, and the continuity of business processes.
- Risks will be identified, assessed, and addressed systematically, establishing security and continuity objectives consistent with the organization's needs and reviewed periodically.

Principle of Awareness and Training

- Training, awareness, and educational campaigns will be implemented for all users with access to information, in order to strengthen the culture of security and continuity within the organization.

Principles of Authenticity, Integrity, Availability, and Traceability

- Authenticity: Ensure that information and systems are used only by those who are duly authorized.
- Integrity: Ensure that information remains complete, accurate, and protected against unauthorized modifications.
- Availability and Continuity: Ensure that information and services are available when needed, safeguarding business continuity through contingency and recovery plans.
- Traceability: Establish mechanisms to properly record and track actions performed on information and systems.

Principle of Accountability

- All Adhara members must take responsibility for their conduct regarding information security and business continuity, complying with established policies, procedures, and controls.

Principle of Continuous Improvement

- Periodic reviews of the management system's effectiveness will be conducted to ensure its suitability and ability to adapt to evolving risks, the technological environment, and business needs.

Principle of Incident and Crisis Management

- Response mechanisms and plans will be established to effectively manage security incidents and crisis situations that may affect the organization, minimizing their impact and ensuring the orderly resumption of activities.