Information Security Policy

Prepared By:	Interfuture Systems Ltd
Prepared For:	Internal
Date:	27/11/2024
Document Ref:	ISMS DOC 5.2
Document Version:	2.0

Purpose

The purpose of this policy is to define the information security policies applicable to Interfuture Systems Ltd that protect the confidentiality, integrity and availability of data.

Scope

All employees

Information Security Policy

Principle
Information security is managed based on risk, legal and regulatory requirements, and business need.

Chief Executive Statement of Commitment

Information processing is essential to our success at Interfuture Systems Lts, and the protection and security of that information is our utmost priority. We have provided the resources to develop, implement, and continually improve an information security management system (ISMS) that is appropriate for our business and compliant with ISO 27001 standards.

Name: David Williams   Signature: Date: 27/11/2024

Introduction
Information security protects the information that is entrusted to Interfuture Systems Ltd. Neglecting our responsibilities pertaining to information security can have significant adverse effects on our customers, employees, reputation, and finances. An effective information security management system enables Interfuture Systems Ltd to:

- Provide Assurance for our legal, regulatory, and contractual obligations
- Ensure the right people have the right access to the right data at the right time
- Protect personal data

Information Security Defined
Information security preserves:

- Confidentiality: Access to information is restricted to those with the appropriate authority

- Integrity: Information is complete and accurate at all times
- Availability: Information is available when needed

Information Security Objectives

To ensure the confidentiality, integrity, and availability of company information based on good risk management, legal, regulatory, and contractual obligations, and business needs.

To provide the resources required to develop, implement, and continually improve the information security management system (ISMS).

To effectively manage third-party vendors who process, store, or transmit information to identify, manage, and mitigate information security risks.

To create a culture of information security and data protection through effective employee training and risk awareness.

Information Security Roles and Responsibilities

Everyone at Interfuture Systems Ltd is responsible for understanding and adhering to established policies and procedures, as well as for reporting any suspected or confirmed breaches. Specific roles and responsibilities regarding the information security management system (ISMS) are defined in the Information Security Roles and Responsibilities document.

Monitoring

Compliance with the policies and procedures of the information security management system are monitored by the Board of Directors, together with periodic independent reviews by internal audits conducted by a third party and external auditors.

Legal and Regulatory Objectives

Interfuture Systems Ltd takes its legal and regulatory obligations seriously. These requirements are recorded in the Legal, Regulatory and Contractual Register.

Training and Awareness

Policies are made readily and easily available to all employees. A training and communication plan is in place to communicate the policies, process, and concepts of information security. Training needs are identified, and relevant training requirements are captured in the Competency Matrix document.

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Technical Director in advance and reported to the Board of Directors.

Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

This policy is updated and reviewed on an annual basis as part of the process for continual improvement.

Issue Date	Version	Detail
09/01/2024	1.0	First Draft
27/11/2024	2.0	Complete redraft of the document which includes CEO commitment.