

---

# INFORMATION SECURITY POLICY

## 1.0. Policy objective

- 1.1. To protect the information assets that Core to Cloud handles, stores, exchanges, processes and has access to, and to ensure the ongoing maintenance of their confidentiality, integrity and availability.
- 1.2. To ensure controls are implemented that provide protection for information assets, and are proportionate to their value and the threats to which they are exposed.
- 1.3. To ensure the company complies with all relevant legal, customer and other third party requirements relating to information security.
- 1.4. To continually improve the company's Information Security Management System (ISMS) and its ability to withstand threats that could potentially compromise information security.

## 2.0. Scope

- 2.1. This policy and its sub-policies apply all people, processes, services, technology and assets detailed in the **Scope**. It also applies to all employees or subcontractors of information security critical suppliers who access or process any of the company's information assets.

## 3.0. Core policy

- 3.1. The company believes that despite the presence of threats to the security of such information, all security incidents are preventable.
- 3.2. The company is committed to achieving the objectives detailed in the policy through the following means:
  - 3.2.1. The implementation and maintenance of an ISMS that is independently certified as compliant with ISO 27001:2022;
  - 3.2.2. The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures;
  - 3.2.3. Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures
  - 3.2.4. The maintenance of a risk treatment plan that is focused on eliminating or reducing security threats;
  - 3.2.5. The maintenance and regular testing of a **Business Continuity Plan**;
  - 3.2.6. The clear definition of responsibilities for implementing the ISMS;
  - 3.2.7. The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties, and can support the implementation of the ISMS;
  - 3.2.8. The implementation and maintenance of the sub-policies detailed in this policy.

- 3.3. The appropriateness and effectiveness of this policy, and the means identified within it, for delivering the company's commitments will be regularly reviewed by Top Management.
- 3.4. The implementation of this policy and the supporting sub-policies and procedures is fundamental to the success of the company's business and must be supported by all employees and contractors who have an impact on information security as an integral part of their daily work.
- 3.5. All information security incidents must be reported to Board of Directors. Violations of this policy may be subject to disciplinary action.

**This document will be reviewed annually**

Signed on behalf of Board of Directors

A handwritten signature in black ink, appearing to read 'P. Howe', with a horizontal line underneath.

Position: CTO

Date: 29/8/25