SECURECORP

INFORMATION SECURITY MANAGEMENT SYSTEM

(ISMS) ISO-IEC-27001

INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

Purpose

The purpose of this Information Security Policy is to establish the framework for maintaining the confidentiality, integrity, and availability of information within Securecorp. It supports the Group's commitment to protecting client data, complying with applicable legal and regulatory requirements — including the *Australian Privacy Act 1988* (as amended), the *Privacy and Other Legislation Amendment Act 2024*, the *Security of Critical Infrastructure Act 2018* (SOCI Act), and the Notifiable Data Breaches (NDB) scheme — and to continuously improving the organisation's Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022.

Scope

This Policy applies to all employees, contractors, and third-party users who access or manage information assets owned, processed, or stored by Securecorp and extends to all locations where Securecorp's business activities are conducted. These assets include physical and digital systems, cloud-based environments (including Software, Infrastructure, and Platforms), artificial intelligence tools, and all information processes and technologies.

Policy Statement

Securecorp's Executive Leadership Team (ELT) are actively committed to upholding the highest standards of information security as a core element of the Group's operational excellence and service delivery. Securecorp recognises that the confidentiality, integrity, and availability of information assets are fundamental to maintaining trust with our clients, stakeholders, and all relevant regulatory bodies.

Accordingly, the following principles guide Securecorp's approach to managing information security:

- Access control shall be based on the principle of least privilege.
- Information shall be classified and handled according to its sensitivity.
- Risk assessments shall be conducted to inform the selection of controls, with particular attention to supply chain and third-party risk.
- All staff shall undergo continuous, role-based security awareness training with particular focus on current threats including phishing, business email compromise, ransomware, and social engineering.
- Cloud services and artificial intelligence tools shall be used in accordance with Securecorp's cloud security and acceptable use standards, reflecting shared responsibility models.
- Security incidents and weaknesses must be reported promptly in accordance with Securecorp's Incident Response Plan and, where applicable, the Office of the Australian Information Commissioner’s (OAIC) NDB scheme's regulatory timeframes.
- Third-party and supply chain risks shall be actively managed in accordance with Securecorp's Third-Party Risk Management framework.

Information Security Objectives

To support Securecorp's commitment to managing information security, Securecorp’s ISMS Committee has established the following objectives:

- Protect information assets from unauthorised access, disclosure, alteration, or destruction.
- Ensure the accuracy and completeness of information and processing methods.
- Maintain the availability of critical systems and data to support business operations.
- Respond promptly to security incidents and breaches in accordance with Securecorp's Incident Response Plan, including meeting the NDB scheme's 30-day assessment requirement where applicable.

- Safeguard all information assets entrusted to Securecorp by implementing robust, risk-based controls that align with ISO/IEC 27001:2022 and other applicable industry best practices and compliance requirements.
- Comply with all applicable legal, regulatory, and contractual requirements, including Australian privacy legislation and sector specific obligations under the SOCI Act.
- Continually improve the ISMS through regular monitoring, review, and ongoing audits or following a significant incident or material change in the regulatory or threat environment.
- Foster a culture of security awareness and accountability across all levels of the organisation through ongoing, role based training, engagement, and performance monitoring.
- Deliver secure, reliable, and cost-effective services that meet or exceed client expectations.
- Ensure all working for and on behalf of Securecorp understand their contribution to the effectiveness and performance of Securecorp's ISMS and the implications of not conforming with Securecorp's information security requirements.

Responsibilities

Securecorp's ELT are responsible for providing strategic direction and resources to support and sustain the implementation and effectiveness of Securecorp's ISMS. In exercising this function, Securecorp's ELT delegate:

a. responsibility for overseeing the implementation, maintenance, and performance of Securecorp's ISMS to the Group's Chief Information Security Officers (CISO), and ISMS Committee; and

b. responsibility for enforcing this Policy and Securecorp's information security expectations to the relevant ISMS Risk Owners and State General Managers.

Information security is a shared responsibility, and accordingly, all who work for and on behalf of Securecorp including employees, contractors, and third parties must comply with Securecorp's Information Security Policy.

Failure to adhere to this Policy

Failure to comply with this policy may result in termination of employment or termination of contract.

Approved by Managing Director
20/01/2025