INFORMATION SECURITY POLICY

Purpose

Coromandel International Limited (hereinafter referred to as “Coromandel”, “the Company”) is committed to safeguarding its information assets and technology infrastructure. Through this Information Security Policy (“the Policy” or “IT Policy”) the Company is committed to protecting its digital assets, ensuring data confidentiality, integrity, availability, and complying with all relevant legal and regulatory requirements. This policy establishes the framework for managing IT resources responsibly and safeguarding information against internal and external threats.

Scope

This Policy applies to all employees, contractors, consultants, and other individuals at Coromandel, including those affiliated with third parties who access Coromandel information processing systems.

Commitment

Coromandel is dedicated to maintaining the highest standards of information security and technology governance. Our commitment includes:

- Safeguard all information assets to maintain confidentiality, integrity, and availability across all operations to ensure integrity and protection of data
- Regularly reviewing and enhancing security controls, technologies and processes to address emerging risks to ensure continuous improvement of information security systems.
- Create a robust monitoring and response framework to identify and mitigate information security threats by implementing proactive monitoring systems and rapid incident response mechanisms to minimize impact.
- Ensuring every employee understands their role in protecting information through clear policies and mandatory training by
- Establishing information security requirements for third parties by defining and enforcing security standards in all supplier and partner agreements to protect Coromandel’s data and systems,
- Adhering to all legal, statutory, and contractual obligations while conducting regular risk assessments to mitigate vulnerabilities.
- Maintaining backup and recovery processes to ensure uninterrupted operations during disruptions.

Roles and Responsibilities

The IT Security Team, led by the CISO, is responsible for overseeing implementation and compliance with this policy. Any amendments shall be placed before the Board/Executive Management for approval. Employees can report any IT security concerns or breaches through the official Helpdesk or a dedicated email channel. All reported issues will be logged, investigated promptly, and resolved in accordance with Coromandel's incident management process, with escalations managed by the Information Security Management Forum (ISMF). Non-compliance with this policy may lead to disciplinary action, including warnings, suspension, termination, or legal proceedings, based on the severity of the violation and in accordance with the company's HR and legal processes.

Training

All employees are required to complete mandatory IT security awareness training during onboarding and attend periodic refresher sessions. These trainings are designed to ensure employees understand acceptable use of systems, maintain strong password practices, and follow proper procedures for reporting security incidents.

Version	Date	Reviewed By	Approved By