# Information Security Policy

The purpose of the Policy is to establish the Port of Townsville Limited's (the Port) commitment to a resilient information and technology environment capable of withstanding, adapting to and rapidly recovering from cyber threats, system failures and adverse events that could disrupt essential Port services. As a critical infrastructure operator, the Port must ensure that its information assets and essential digital systems, remain secure, reliable and resilient.

This Policy sets the principles and expectations that underpin the Port's Information Security Management System (ISMS) and supports compliance with ISO 27001:2022. It applies to all information assets, systems, technologies and services owned, operated or managed by the Port, including those delivered or supported by third-party providers.

The Port is committed to maintaining a proactive and resilient cyber security posture that:

- Anticipates emerging threats through continuance monitoring, risk assessment, and situation awareness.
- Withstands cyberattacks and disruptions through layered defence in depth controls, secure architectures, hardened systems and robust governance.
- Detects and responds to cyber incidents promptly to minimise operational impact.
- Recovers essential services within acceptable timeframes following a disruption.
- Continuously improves resilience by regularly testing Business Continuity, Disaster Recovery and Cyber Incident Response processes.
- Builds a strong cyber security culture through ongoing training, communication and leadership engagement

In support of this posture, the Port's Information Security Management System (ISMS) Objectives are:

- Protect the Confidentiality of information from unauthorised access, disclosure or misuse.
- Ensure the Integrity of information (its accuracy and completeness) is safeguarded against unauthorised modification or destruction.
- Maintain availability so information systems and critical services remain accessible, resilient and dependable in line with business and operational requirements through appropriate risk management activities.
- Legal regulatory and contractual requirements relating to information security are identified and understood.
- Maintain and test Business Continuity, Disaster Recovery and Cyber Response plans to ensure critical services can be sustained or restored within acceptable timeframes.
- Promote Information security awareness by providing appropriate resources and guidance to all employees and contractors.
- Ensure all cyber security incidents are reported, investigated and responded to promptly in accordance with the Port's incident response playbooks.
- Ensure the documentation necessary for the effective implementation of this Policy, including standards, procedures and guidelines is developed, maintained and kept current.

The following roles and responsibilities support the Port cyber security resilience and the effective implementation of this policy.

- Executive Management holds overall accountability for information security and cyber risk, including setting expectations, approving risk appetite, and ensuring appropriate governance and resourcing are in place.
- The Manager Information and Digital is accountable for the effective management of information security and cyber risks including ensuring appropriate controls, oversight and escalation of material risks.
- The Cyber Security Lead is responsible for providing specialist oversight, advice and coordination in relation to information security and project -related cyber risks, including supporting risk identification, assessment and treatment.
- The Supervisor, Technology Services is responsible for the implementation and day-to-day management of operational security practises and system-level controls within the technology environment.
- It is the responsibility of each employee and contractor to adhere to comply with the Information Security Policy and all supporting standards and procedures.

This policy will be reviewed following significant legislative, regulatory or organisational changes, or at a minimum, every three years to ensure ongoing suitability and effectiveness.

**RANEE CROSBY**
**CHIEF EXECUTIVE OFFICER**