Information Technology and Security Policy

Purpose and Scope

The Information Technology and Security Policy specifies and explains the minimum standards for implementing IT security policies and procedures within The Centre and establishes the foundation for practices that regulate access to The Centres IT systems and the information processed, stored, and transmitted by those systems.

This policy applies to all departments and their employees, contractors, guests, collaborators, and any other personnel requiring access to the systems, networks, devices, software, data or media, that constitute The Centre's IT platform.

Policy

The Centre is committed to implementing an Information Security Management System (ISMS) to ensure information systems are appropriately protected from loss of confidentiality, integrity, and availability

Our commitment is to ensure that The Centre

- Implement and maintain an effective ISMS
- Maintain systems to ensure integrity and protection against unauthorised alteration or destruction
- Ensure employees and users have timely and reliable access to information and services
- Promote security of information and information systems
- Employees understand the importance of information security and comply with all policy, procedures and standards regarding information and information assets
- Align risk management practices relating to the ISMS with International Standards Organisation (ISO) 27001:2013
- Implement controls for identified risks, threats and vulnerabilities
- Set a baseline for information security and continue to improve the management system
- Complies with statuary, legislative and government direction regarding information security

- Communicates appropriately and timely to all stakeholders who use or are impacted by The Centre's ICT platform and security measures.

A Chief Information Officer (CIO) shall be appointed to provide cyber security leadership and guidance for their organisation. Unless otherwise documented, the GM Business Operations shall act as the CIO.

Whilst the responsibility for management and security of the ICT platform is an operational responsibility, the Board Risk and Governance Committee shall have oversight of the platform's security performance and evaluation of the ISMS effectiveness.

Definitions

Term	Definition

Version Control

Policy Operative From	27/07/2022	**Date and Current Version**	Version 1.0 27/07/2022
Responsible Officer	GM Business Operations	**Policy Approved By**	CEO
References	• Cyber Incident Response Plan Guidance and Template, Australian Cyber Security Centre (Dec 2021) • Cyber Incident Response Readiness Checklist, Australian Cyber Security Centre (Dec 2021) • The Privacy Act (1998)	**Related Policy**	• Information Privacy and Data Security Policy • Information Technology Acceptable Usage Policy • IT Fair and Safe Use Policy • Records Management Policy • Social Media Policy
Related Procedure	• Information Technology and Security Procedure • Data Breach and Response Plan Procedure	**Related Document, Forms or Guidelines**	• Information Technology and Security Emergency Response Plan • The Centre Emergency Response Plan