Cyber Security Policy

Policy statement

CS Energy will seek to protect the confidentiality, integrity and availability of its technology and information assets. This target aims to safeguard our people our business and our customers, whilst maintaining compliance and alignment with government and industry requirements.

Objectives and principles

Our policy objectives are to:

- Design and deliver Security practices that, improve our technology and information resilience and reduce risk in alignment with our corporate risk appetite.
- Maintain and embed a corporate culture of awareness around technology and information security.

We will achieve this through the application of following principles across all technology and information assets:

- **Risk Based:** Ensure technology and information related security decisions, controls and procedures mitigate risk within the defined risk appetite.
- **People Centric:** Develop an effective security culture through ongoing information security and awareness training.
- **Business-aligned:** Ensure technology and information security controls, processes and procedures are fit for purpose, supports a safe environment and return appropriate value to the business.
- **Secure by Design:** Ensure technology investments are selected, implemented, managed and maintained throughout their lifecycle incorporating appropriate security requirements.
- **Defence in depth:** Implement a multi-layered strategy for technology and information security that can flex to identify, detect, protect, respond and recover from threats and risk of compromise.
- **Response and Recovery:** Implement people, processes and systems that enable response to security incidents and ensure recovery in a timely and effective manner.

Scope

This policy applies to:

- CS Energy employees, contractors and consultants.
- CS Energy business partners, third party providers and their affiliates.
- CS Energy information and technology assets, which includes both corporate (IT) and operational technology (OT) systems, assets and services.

Responsibilities

Every person working for CS Energy is required to actively participate in the implementation of and adherence to this policy.

- The CS Energy Board, Chief Executive Officer, Executive Leadership Management Team and Technology Leadership Team are responsible for ensuring that technology and information security objectives are met.
- The Chief Information Officer is responsible for implementation and review of this policy.

Actions

CS Energy's actions to support this policy are to establish and maintain:

- Appropriate technology governance.
- Practices that deliver technology, information security management and awareness.
- Leadership engagement and support for a structured Program of work delivering improvement initiatives designed to reduce cybersecurity risk across OT and IT systems, assets, and services.
- Compliance with regulatory and legal obligations.

Cyber Security Framework

CS Energy commits to aligning our Cyber Security Policy and related technology and information standards with the following frameworks to achieve the objectives and principles:

- Australian Energy Sector Cyber Security Framework (AESCSF)
- International Standards Organisation 27001 Information Security Standard (ISO 27001)

May 2022