Business Resilience Policy

Policy statement

Organisational resilience is the ability of an organisation to anticipate, prepare for, and respond and adapt to business disruptive events (ISO22316:2017 Organisational Resilience and Part 2A of the Security of Critical Infrastructure Act 2018). CS Energy will maintain an organisationally appropriate business resilience framework to ensure business continuity is maintained at all times. The Corporation will develop, enhance and regularly review the plans, procedures and systems put in place to safeguard the Corporation's assets and personnel from natural and manmade disaster and threats. The Business Resilience Framework will enable the organisation to effectively respond to, manage and recover from business disruptive events.

Principles and Objectives

To minimise the impact that a major disruption could have on the viability of the organisation. This includes:

- Ensuring the welfare of staff, contractors and the community
- Protecting the organisation's image and reputation
- Maintaining a level of stakeholder satisfaction
- Enhancing organisational stability
- Reducing risk exposures and potential impacts
- Creating resilience through comprehensive procedures to plan for and manage multiple and varied incidents
- Ensuring continuity of critical services and critical supplies during any incident
- Minimising legal liabilities
- Anticipating and satisfying future regulatory requirements

Scope

This Policy describes the principles for Business Resilience across CS Energy and applies to all site and Corporation activities.

Business Resilience includes Crisis Management, Business Continuity Management, Critical Incident Management, Communications Response and IT Disaster Recovery.

Responsibilities

Effective governance enables the exploitation of opportunity and mitigation of risk and ensures appropriate people and teams are accountable for decisions (BS65000:2014). It will also include maintenance of records pertaining to all validation and review activities.

The Senior Leadership Group are ultimately accountable for ensuring Business Resilience is considered during decision making and change management activities, and an appropriate level of resilience is achieved by the organisation.

Actions

The Policy will be carried out through processes, systems and capability incorporating the following key business continuity management elements.

- **Vulnerability and Risk Assessment**
  CS Energy will apply accepted risk management methodologies and impact analysis to identify vulnerabilities, risk levels and impacts to production, physical and non-physical assets and the community associated with natural/manmade disasters and malicious threat including cyber and biological threat and terrorism.
  Identify potential hazards where there is a material risk that the hazard occurrence could have a relevant impact on the asset and as far as it is reasonably practicable, minimise or eliminate any material risk of such a hazard occurring.
- **Response Capability**
  A capability to respond to all incidents and circumstances will be maintained and involve impact analysis, specific response plan development and activation, resources to implement a plan and roles, responsibilities and authorities to act in relation to the plan. So as far as it is reasonably practicable to do so, mitigate the relevant impact of a hazard on the assets and processes of the business. Guidelines and systems will be in place for the management and reporting of security incidents and to support the response to terrorist threat or change in the national counter-terrorism alert level.
- **Emergency/Crisis Management**
  An Emergency/Crisis Management Plan will be maintained, regularly reviewed, tested and cover a full range of threat scenarios.
- **Communications**
  Key communication channels for crisis/emergency management will be identified, formalised and be regularly reviewed and tested.
- **Physical Security of CS Energy Sites**
  Site physical security will be managed and controlled through Site guidelines and procedures and security arrangements. Site physical security will be consistent and variable with advised threat levels and will be regularly reviewed and inspected to assess compliance.
- **Information Technology and Cyber Security**
  A security regime addressing all aspects of IT security and disaster recovery (plan, procedure, resource and strategy) will be maintained and tested regularly.
- **Personnel Employment and Training**
  Sound processes will be maintained to ensure the employment of reliable and appropriately qualified people. Appropriate training in security matters will be provided.
- **Protecting Potentially Sensitive Information**
  Principles for the release of such information shall apply.
- **Validation and Review Schedule**
  CS Energy will undertake regular validation activities to demonstrate the efficacy of its program and identify opportunities to strengthen the program when required in order to better understand its resilience capability.
- Validation and reviews will occur annually, or following a significant material, operational or structural change.

October 2023