central
highlands
COUNCIL

Policy No. 2019 - 56

Cybersecurity Policy

Background

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorised access. Protection of information, systems and services is critical to effective delivery of council's services, and maintenance of public confidence in these services.

Purpose

The purpose of this policy is to provide a consistent, risk-based approach to protecting Central Highlands Council information, systems and services from cybersecurity threats.

Benefits

The policy:

- improve council's ability to identify and respond to cybersecurity risks;
- improve cybersecurity risk management;
- raise cybersecurity awareness among staff;
- increase confidence in council's digital services;
- integrate cybersecurity risks into our risk management framework; and
- enable increased information sharing with all levels of government and relevant external organisations.

Policy statement
Central Highlands Council will identify and manage cybersecurity risks to its information, systems and services.

Policy principles
Central Highlands Council Cybersecurity Policy is founded upon the following underlying principles.

- AWARENESS

Increased cybersecurity awareness enables staff at all levels to understand their responsibilities and identify and respond to cybersecurity risks.

- COLLABORATION

Sharing cybersecurity knowledge across organisation improves cybersecurity capability and maturity.

- ENABLEMENT

Cybersecurity is a key enabler for digital transformation.

- INTEGRATION

Integrating cybersecurity into the risk management framework, policies and procedures improves planning for, and responses to cybersecurity incidents.

- PRIVACY AND SECURITY

Integrating cybersecurity into all digital systems and services improves privacy and security for consumers of Central Highlands Council services.

- RISK

Adopting a risk-based approach allows the council to adapt its cybersecurity risk management approach based on its risk tolerance.

- STANDARDS

Aligning with national and international industry standards provides a consistent, systematic and repeatable approach enabling collaboration across government and the private sector. Applicable international standards are AS ISO/IEC 27001 for cybersecurity management requirements and AS/NZS ISO 31000 and AS/NZS ISO/IEC 27005 for risk management.

Responsibilities

Each Manager is responsible for ensuring their department identifies and manages cybersecurity risks. This includes:

1. Taking a risk-based approach to the management of cybersecurity practices, including the management of any risks associated with the cybersecurity practices of service providers engaged by the organisation;
2. Contributing to the development and refinement of Council's Cybersecurity practices;
3. Providing timely notification to the General Manager of cybersecurity events and incidents that could impact public confidence or affect the delivery of Council's services; and
4. The General Manager is to report annually to the Audit Committee on any cybersecurity events and incidents that could impact public confidence or affect the delivery of Council's services, including the mitigation of cybersecurity risks.

Definitions

Cybersecurity	The body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorised access
Cybersecurity Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Cybersecurity Incident	A single or series of unwanted or unexpected cybersecurity events that have a significant probability of compromising business operations and threatening information security
Service Provider	An organisation, business or individual that provides services or products to council
Risk	Effect of uncertainty on objectives
Risk Management	Overall process of risk identification, risk analysis and risk evaluation
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk tolerance	An organisation's readiness to bear the risk in order to achieve its objectives
Risk-based	Prioritised decision-making according to the risk level and the risk tolerance of the organisation