Date: Juy 2026
Business unit: Technology Innovation

Information Security Policy and Governance Principles

Purpose

The purpose of this policy is to ensure that Contact personnel, contractors and relevant third parties understand Contact's expectations for protecting information, technology and operational systems.

The policy establishes the principles that support the management of information security risk and the protection of information and technology assets in a manner consistent with Contact's risk appetite, governance framework and business objectives.

Application

This policy applies to all persons, including Contact employees, contractors and third parties who are involved in the use, design, procurement, delivery, management or support of Contact information, technology systems or digital services. The policy applies to information, technology systems, operational technology and supporting business services used to support Contact's operations and strategic objectives.

Non-Compliance

Information security requirements are established to protect Contact people, information, assets and services. Where compliance with a requirement is not possible, the associated risk must be assessed and managed through approved governance and risk management processes. Any exceptions must be appropriately reviewed, documented and approved by the relevant business owner in accordance with Contact's governance requirements.

1. Information Security Governance

Information security forms part of Contact’s broader risk management and governance framework. The Board maintains oversight of material cybersecurity and information security risks through the Audit and Risk Committee. Executive accountability for information security is supported through governance processes, policies, standards, security management activities and risk reporting.

2. Security Awareness and Culture

Contact recognises that security is a shared responsibility. Security awareness and education activities are maintained to help employees, contractors and relevant third parties understand security expectations, recognise cyber threats, protect information appropriately and contribute to a strong culture of security and resilience across the organisation.

3. Information Security Incident Management

Contact maintains processes to support the identification, reporting, assessment and management of information security incidents, vulnerabilities and suspicious activity. Employees, contractors and relevant third parties are expected to promptly report suspected information security incidents through approved reporting channels, and information gained through incident management activities is used to strengthen resilience and improve security practices over time.

4. Business Continuity and Resilience

Information security supports Contact's broader business continuity and resilience objectives through the protection of information, technology systems and critical services. Security considerations are integrated with business continuity, disaster recovery and resilience activities across the organisation to help reduce the likelihood and impact of events that could affect Contact's operations.

5. Information Security Risk Management

Contact applies a risk-based approach to managing information security risks. Information security risks are identified, assessed, treated and monitored throughout the lifecycle of information systems, technology services and operational environments. Security considerations are integrated into technology change, supplier engagement and business operations to support an acceptable level of risk for the organisation

6. Information Security Strategy

Contact maintains a strategic approach to information security that supports critical operational and business outcomes. Information security priorities are informed by business risk, technology change, emerging threats, assurance activities and strategic objectives, and are delivered through Contact's Cybersecurity Management Programme and broader technology strategy.

7. Publication Note

This public version has been prepared to support external transparency and sustainability disclosure. Detailed technical security requirements, implementation standards and operational procedures are maintained internally and are not published for security reasons.