Cybersecurity at Contact Energy

Contact Energy is committed to maintaining the security and resilience of the technology, information and operational systems that support our business, customers, people and generation assets. We recognise that cybersecurity is an ongoing business responsibility. It supports reliable operations, protects information, enables safe technology change and helps maintain the trust of our customers, communities, partners, investors and regulators.

Our approach to cybersecurity combines governance, accountable leadership, risk management, security operations, awareness and education, assurance and continuous improvement.

Governance and accountability

Cybersecurity forms part of Contact's broader risk management and governance framework.

Our Board maintains oversight of material technology and cyber risks through the Audit and Risk Committee. Regular reporting supports oversight of cyber risk, programme delivery, significant incidents, assurance activity, emerging threats and improvement priorities.

Executive accountability for cybersecurity sits within Contact's technology leadership structure. Cybersecurity is supported by internal governance, policies, standards and risk management processes that help ensure cyber and information security risks are considered consistently across the organisation.

Contact31+ and our Technology strategy

Contact31+ recognises technology as a key enabler of business performance, customer outcomes and operational resilience. Cybersecurity supports this strategy, ensuring systems are stable, secure and able to support safe growth.

Our Technology strategy includes a focus on stable and secure systems, alongside advanced data and AI, and simpler, more flexible technology. Cybersecurity contributes to this by reducing material cyber risk, strengthening resilience and supporting secure technology delivery across Contact.

Security is embedded into technology planning, architecture, delivery and operational improvement activity so Contact can modernise safely and adapt effectively to changes in the external threat environment.

Security across technology and operational environments

Contact's cybersecurity approach applies across information technology, operational technology and the digital services that support our customers, people and business operations.

Our programme is risk-based, with focus areas prioritised according to the criticality, threat environment, assurance findings, technology change and potential impact on customers, operations and the business.

We maintain a focus on identity and access, detection and response, vulnerability management, operational resilience, supplier security, secure technology delivery and protection of critical systems.

Artificial intelligence and emerging technologies

Contact's cybersecurity governance extends to new and emerging technologies, including artificial intelligence. AI-enabled systems and services are considered through governance, risk and security processes that support responsible use and help manage privacy, security, regulatory and operational risks.

Our approach aims to enable Contact to realise value from AI while applying appropriate oversight, accountability and control to AI-enabled technology.

Security awareness and education

Cybersecurity is a shared responsibility across Contact.

We maintain a security awareness and education programme to help ensure our people understand emerging cyber threats, recognise suspicious activity, protect information appropriately and contribute to a strong security culture across the organisation.

Assurance and continuous improvement

Contact regularly assesses its cybersecurity maturity and control environment to identify improvement opportunities and inform future investment.

Assurance activity, maturity assessment, security testing, operational learnings and changes in the threat environment are used to shape the cybersecurity roadmap and prioritise improvement activity.

This supports an adaptive and intelligence-driven cybersecurity capability aligned to business strategy, risk appetite and the need to operate securely in a changing energy sector.

Cybersecurity is an important part of Contact's ability to operate safely, reliably and responsibly. We continue to invest in people, processes, technology and assurance to strengthen resilience, protect information and support the secure delivery of Contact's strategic priorities.