ICT001 Information Security

Purpose

The objective of this policy is to manage the information security of Echo Australia Inc (Echo) and to ensure that its core and supporting business operations continue to operate with minimal disruptions whilst maintaining the integrity, confidentiality and availability of information.

Management is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets throughout the company and entrusted to it by the Department of Employment and Workplace Relations, the Department of Social Services, its participants and other stakeholders, whilst ensuring all of our legislative obligations are met.

Policy

To achieve this, the policy of Echo is to establish and maintain an efficient and effective Information Security Management System that is planned, developed, communicated and integrated within the business functions of the organisation. This is to protect the organisation's information assets from all threats, whether internal, external, deliberate or accidental.

Echo's Information Security Management System is based on the requirements of AS/NZS ISO 27001 and selected ISM controls as identified by the Department of Employment and Workplace Relations.

As part of this policy, we ensure:

- Compliance with applicable business, legislative and regulatory requirements and contractual security obligations.
- Continuity of business operations in the event of a crisis or disaster through the formulation, maintenance and periodic testing of Echo's Business Continuity Plan.
- All breaches of information security, actual or suspected, are reported to and investigated and where applicable notified to relevant regulatory authorities and other interested parties.
- Information and IT related risks are identified, assessed and controlled according to our formal Risk Management process with the aim to eliminate or minimise risk, or in the worst-case scenario adequately control risk.
- Contractors and third parties working on our behalf are required to comply with Echo ICT policies and procedures to ensure that the confidentiality, integrity and availability requirements of all information systems are met.
- Information security education, awareness and training is made available to employees, applicable contractors and third parties.
- Appropriate access control is maintained and information is protected against unauthorised access or modification.
- Continually improve the Information Security Management System through the establishment and regular review of measurable security objectives at relevant functions and levels of the organisation.
- A documented Statement of Applicability is maintained and regularly updated.
- The appropriate handling of information is based on minimum handling requirements, classifications or other information control markers.

All managers at Echo are responsible for implementing ICT Policies within their teams and for adherence by their employees. It is also the responsibility of each employee to adhere to ICT Policies.

As the business needs change, we are committed to ensuring our management system remains flexible to continually meet our evolving requirements. This is achieved through the regular review of objectives and ICT Policies and procedures.

Michael Locke
Chief Executive Officer
June 2026