ICT001 - Information Security Policy

Document Classification: Unofficial
Audience: Public

Objective

echo's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions whilst maintaining the integrity and confidentiality 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 Education, Skills and Employment, the Department of Social Services, its clients 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 organization's information assets from all threats, whether internal or 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 Education, Skills and Employment.

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 The 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;
- Require contractors and third parties working on our behalf 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 staff, applicable contractors and third parties;
- Appropriate access control is maintained and information is protected against unauthorized 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 units and for adherence by their staff. It is also the responsibility of each member of staff to adhere to ICT Policies.

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

Michael Locke
Chief Executive Officer
November 2023