Information Security Policy
Information Security

Reference number	ICT.001	**Policy owner**	Chief Information Officer
Contact officer	Chief Information Officer	**Contact details**	[redacted]
Version	1.2	**Approved by**	[redacted]
Effective date	27/05/2025	**Review frequency**	Annual

Purpose

This policy specifies the commitment of the Department of Trade, Employment and Training (DTET) to manage its approach to information security in accordance with the Queensland Government Customer and Digital Group (QGCDG) Queensland Government Enterprise Architecture (QGEA) Information Security Policy (IS18:2025).

DTET's core security requirement is to provide assurance to all interested parties that it manages its information, the information entrusted to it, and its ICT assets, to protect against unauthorised use or accidental modification, loss or release.

Policy

To meet this requirement, we are committed to the following security objectives:

- Provide a structured approach to information security management that is consistent throughout DTET and is cognisant of the need to manage commercial and reputational risks, while ensuring ongoing stakeholder trust and the delivery of services.
- Maintain the confidentiality, integrity and availability of information assets in compliance with policy, legal and regulatory requirements including QGCDG guidelines.
- Implement effective information security controls to ensure adequate protection of DTET information assets.
- Establish a consistent and flexible approach to the assessment, management and treatment of information security risks.
- Continual improvement of the information security practices of DTET.
- Maintain a high level of security awareness amongst DTET personnel by emphasising that everyone has responsibility and accountability for the protection of information.
- Obtain assurance that external third parties are appropriately managing and securely exchanging DTET information.
- Monitoring systems and investigating all detected security breaches and weaknesses.

Scope

This policy encompasses:

- All information owned by or under the control of DTET; and
- Information in both physical and electronic form.

The requirements and expectations outlined in this policy apply equally to all users defined as:

- All fulltime, part time, temporary or casual DTET employees and volunteers;
- All contractors engaged by DTET; and
- All suppliers providing services to DTET.
- Any other third parties with a valid reason to access DTET information

Roles & Responsibilities

Role	Responsibility
Board of Management	Reviews this policy.
Information Security Working Group	Reviews and endorses this policy
Director, ICT	The provision and implementation of IT assets and processes that have effect to this policy. The establishment and maintenance of monitoring and compliance systems and processes to ensure that the supporting mechanisms are functioning effectively.
Regional Directors	To provision and implement the physical security of DTET sites and Information Assets within their region.
Managers and Supervisors	Advising users of their obligations under this policy, monitoring and where necessary enforcing the policy.
Employees, contractors and third parties	Administering ICT controls in place to protect DTET information assets and maintaining controls within the requirements set by this policy.
All users	Ensuring appropriate use of DTET information assets, as well as undertaking relevant training such as mandatory code of conduct training, and other training relating to this policy where appropriate.

Reference Documentation

This policy will be read in conjunction with:

- DTET Information Security Framework
- Information Security Standards ISO/IEC 27001:2022 and ISO/IEC 27002:2022;
- QGCDG Information Security Policy IS18:2025;
- Queensland Government Information Security Classification Framework;
- Public Records Act 2023;
- Privacy Act 2009.

Compliance and Enforcement

Failure to comply with any element of this policy may result in disciplinary action, up to and including termination of employment in accordance with DTET's disciplinary process and the Code of Conduct for the Queensland Public Service.

Exemption from this policy must be sought in writing from the Chief Information Officer.

Policy Review

This policy shall be subject annual review or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. Reviews shall incorporate:

- Assessment of opportunities for improvement of DTET's approach to information security; and
- Consideration of changes to the organisational environment, business circumstances, legal conditions, or the technical environment.

Version History

Date	Version	Description of Modification	Modified By
23/09/2019	1.0	Approved by DG after ISC endorsement	[redacted]
02/09/2022	1.1	Standard review	[redacted]
26/05/2025	1.2	Update of template and change of department name	[redacted]
27/05/2025	1.2	Approved by CIO – CM Ref F25/114	[redacted]