July 2026

Information Security Policy

Version 3.0

QUEENSLAND Family & Child Commission

Queensland Government

1. Objective

This policy outlines the principles, objectives and approach to managing information security within the Queensland Family and Child Commission (the Commission).

The Commission will implement security controls to protect the information it holds by applying a systematic and repeatable approach to information security and integrating this policy into corporate risk management processes. This will ensure business continuity and the adoption of recognised international and Australian standards to managing information security.

1.1 Scope

This Information Security Policy applies to the protection of all Commission information, application and technology assets. This includes electronic and hard copy assets owned by the Commission and/or entrusted to it by customers, partners or external third parties.

This policy applies to all Commission employees, sub-contractors or consultants and any external parties deployed or engaged within the Commission.

This policy encompasses all forms of accessing, storing and distributing information to the Commission. As such, the policy applies to on-site and off-site (remote) Commission work arrangements (e.g. home-based, mobile, regional, and interstate).

The Commission implements and operates an ISMS based on ISO 27001, consistent with IS18 Requirement 1, covering services, information, applications and technology assets across the organisation and its suppliers.

2. Legislative and regulatory requirements

- all Commission ICT assets are assigned appropriate controls in accordance with the ***Queensland Government Information Security Classification Framework*** **(QGISCF)**
- all PROTECTED and SENSITIVE information in transit and at rest is encrypted in accordance with the ***Data Encryption Standard*** **(DES)**
- all services requiring user authentication are guided by the ***Queensland Government Authentication Framework*** **(QGAF)**, and
- the Australian Signals Directorate (ASD) ***"Essential Eight" Strategies to Mitigate Cyber Security Incidents*** are implemented.
- ***Information Privacy Act 2009 (Qld)***
- ***Finance and Performance Management Standard 2019***
- ***Queensland Government Enterprise Architecture***

3. Principles

The principles of this policy include:

- Adopt systematic and repeatable information security management practices.
- Protect the confidentiality, integrity and availability of Commission information assets.
- Comply with applicable Queensland Government information security frameworks and standards.
- Implement appropriate security controls and obtain ongoing assurance of their effectiveness.
- Maintain accountability and governance through regular attestation and reporting.
- Report information security incidents in accordance with government requirements.
- Ensure information security aligns with relevant legislation, policy and risk management frameworks.

- Promote shared responsibility for information security across all staff and third-party partners.

4. Policy

The Commission is responsible for managing a significant amount of information held in both electronic and paper-based formats. Protecting this information is essential to maintaining public trust, ensuring operational integrity and meeting statutory obligations. As a statutory body captured under the *Financial and Performance Management Standard (FPMS) 2019*, the Commission must have regard to the *Information and cyber security policy (IS18)*, which forms part of ***Queensland Government's Enterprise Architecture*** **(QGEA)**.

The purpose of this policy is to outline the information security requirements necessary to safeguard Commission information assets. This includes ensuring that all systems, processes, and technologies that create, process, store, view or transmit information, are protected against any unauthorised access, misuse or accidental modification, loss or disclosure. The policy also ensures that the Commission implements information security controls aligned with IS18 and recognised industry standards, supported by effective governance, risk-based decision making, and consistent organisation wide practices to maintain confidentiality, integrity and availability of Commission information.

4.1 Applying the requirements of IS18

As a statutory body captured under the **Financial and Performance Management Standard (FPMS) 2019**, the Commission must have regard to IS18 and apply its requirements where relevant.

The following requirements translate IS18 obligations into clear, actionable expectations for the Commission:

1. **Information Security Management System (ISMS)** – The Commission is aligned to ISO 27001, consistent with the requirements of IS18. This provides the overarching framework for managing information security across all services, information assets, applications and technologies, ensuring a structured and coordinated approach to safeguarding Commission information.
2. **Security Risk Management** – Information security risks are managed through a systematic and repeatable process that is embedded within the Commission's broader corporate governance and risk management arrangements. Officers are required to identify, assess and monitor security risks relevant to their areas of responsibility, ensuring that these risks are addressed in a manner consistent with the Commission's risk appetite and responsive to the evolving threat environment.
3. **Minimum Information Security Requirements** – The Commission applies the mandatory minimum information security requirements mandated under IS18, including classification of information in accordance with the **Queensland Government Information Security Classification Framework** (QGISCF), encryption of protected and sensitive information under the **Data Encryption Standard** (DES), authentication aligned with the **Queensland Government Authentication Framework** (QGAF), and implementation of the **Australian Signals Directorate (ASD)** **Essential Eight strategies** to mitigate cyber security risks.
4. **Security Assurance for Information Systems** – Information systems used by the Commission are subject to appropriate security assurance activities, including reviews, assessments and other verification measures that evaluate the design and effectiveness of implemented controls. These assurance processes support informed decision-making, provide transparency over risks affecting systems and services, and contribute to the Commission's overall security posture.
5. **Information Security Attestation** - The Commission is required to provide annual attestation of its information security arrangements, confirming that they are appropriate and aligned to risk, legislative obligations and IS18 requirements. Officers contribute to this process by ensuring that relevant information, evidence and documentation regarding security controls, risks and system performance is accurate and complete.
6. **Information Security Annual Return** – The Commission is required to complete an Information Security Annual Return each year, outlining its compliance with IS18 and associated QGEA standards. Officers

must ensure that reporting inputs and supporting materials accurately reflect the Commission's information security measures, risks and overall maturity.

7. **Information Security Incident Reporting** - Information security incidents must be identified, recorded and reported in accordance with the Queensland Government Information Security Incident Reporting Standard. Officers have a responsibility to escalate suspected incidents promptly so that appropriate containment and response actions can be undertaken.
8. **Mandatory Notification of Data Breaches (MNDB)** - Suspected eligible data breaches must be assessed within statutory timeframes, logged in the internal data breach register, and notified to affected individuals and the Office of the Information Commissioner (OIC) where serious harm is likely. Officers are expected to report potential breaches immediately and contribute to the assessment and documentation processes to ensure compliance with MNDB obligations. See the Commission's MNDB Policy and MNDB Procedures for more detail on obligations and processes.
9. **Consistent Organisation-Wide Security Practices** - Information security practices must be applied consistently across the Commission, supported by approved policies, procedures, governance arrangements and training. Officers are responsible for handling information in accordance with security and classification requirements, applying appropriate controls, and participating in activities that support the Commission's secure operating environment.
10. **Continuous Improvement and Cyber Resilience -** The Commission maintains a commitment to continual improvement of its information security capability. This involves regularly reviewing and updating controls, incorporating lessons learned from incidents and assurance activities, monitoring compliance and responding to changes in risk, technology and threat conditions. Officers contribute to strengthening cyber resilience by adopting secure practices, supporting assessments and maintaining awareness of information security responsibilities

4.2 Queensland Privacy Principles (QPPs)

In addition to information security obligations, the Commission must also comply with the privacy requirements established under the ***Information Privacy Act 2009 (Qld)***. **The Queensland Privacy Principles** (QPPs) set the standards for how the Commission collects, manages, uses, and discloses personal information. Together, IS18 and QPPs ensure that the Commission's information management practices protect both the security and privacy of information throughout its lifecycle. The Commission adheres to the **Queensland Privacy Principles**.

Relevant to the Commission's work are:

QPP 1: Open and transparent management of personal information

The Commission will maintain practices, procedures and systems to ensure QPP compliance and will publish an up-to-date, clearly expressed privacy policy that is available free of charge and in an appropriate form.

QPP 2: Anonymity and pseudonymity

Where lawful and practicable, the Commission will provide options for individuals to interact anonymously or using a pseudonym.

QPP 3: Collection of solicited personal information

The Commission will only collect personal information that is reasonably necessary for, or directly related to, its functions, by lawful and fair means; higher standards apply to sensitive information (for example consent unless a lawful exception applies).

QPP 4: Dealing with unsolicited personal information

The Commission will assess unsolicited personal information; if it could not have been lawfully collected and is not a public record, it will be destroyed or de-identified where lawful and reasonable.

QPP 5: Notification of the collection of personal information

At or soon after collection, the Commission will take reasonable steps to notify individuals of required matters (purpose, legal authority, likely disclosures, access/correction processes, and consequences of not providing information).

QPP 6: Use or disclosure of personal information

The Commission will use or disclose personal information only for the primary purpose of collection or as permitted by law (including with consent or where a permitted secondary purpose applies) and will maintain appropriate records of disclosures.

QPP 10: Quality of personal information

The Commission will take reasonable steps to ensure personal information is accurate, complete, up to date and relevant before use or disclosure.

QPP 11: Security of personal information

The Commission will protect personal information against loss, unauthorised access, misuse, modification and disclosure and will destroy or de-identify personal information when no longer required and when lawful to do so.

QPP 12: Access to personal information

The Commission will provide individuals with access to their personal information unless a lawful exception applies, via timely and transparent processes.

QPP 13 Correction of personal information

The Commission will take reasonable steps to correct personal information that is inaccurate, incomplete, out of date or misleading.

5. Delegations and other role responsibilities

Role	Responsibilities
Principal Commissioner	Be the accountable officer responsible for ensuring all Commission employees are compliant with the Information Security Policy (this document). Be the accountable officer responsible for ensuring that the Commission meets its reporting requirements.
Chief Operating Officer	Overseeing organisation-wide implementation of the ISMS. Operationalise the governance framework for information security across business units, ensuring controls are designed, implemented and monitored in operations Ensure financial information systems and supporting ICT meet security, integrity and availability requirements and have regard to QGEA
Executive Directors	Ensure divisional controls for information security and privacy are implemented and operating effectively within their portfolios Enforce MNDB processes in their divisions
Executive Leadership Board	Providing organisation-wide governance for information security. Setting the Commission's strategic direction for cyber and information security. Reviewing and endorsing significant information security risks. Seeking regular reporting on system security, threats and emerging risks.
Directors	Ensuring information assets under their authority have appropriate security classifications. Managing and escalating information security risks. Implement controls over information assets, including classification, access and retention practices in line with organisational policy and QGEA-aligned standards adopted by the Commission Manage local risk registers for information/cyber risks and ensure treatments are executed and monitored Trigger and document MNDB steps at the team/system level when events occur
Managers	Ensuring staff complete required training and understand policies. Supervising day-to-day adherence to information security controls. Escalate incidents and suspected data breaches immediately and support containment and assessment activities. Provide evidence for audits/assurance (e.g., control checklists, logs) that underpin FPMS governance and reporting.

Role	Responsibilities
	Handle personal information lawfully and fairly in line with the QPPs. Follow approved controls and procedures for information security that form part of the Commission's internal control structure Report suspected data breaches immediately to enable MNDB timelines to be met
All staff	All staff contribute to compliance with this document by understanding and following all information security policies, procedures and controls. Reporting security incidents immediately. Maintaining vigilance and cyber hygiene. Supporting assurance and compliance activities i.e. audits, risk assessments.

6. Considerations

6.1. Consideration of Human and Child Rights

The policy upholds:

- Right to privacy and reputation
- Right to equality before the law and non-discrimination
- Right to recognition and equality before the law (procedural fairness)
- Right to take part in public life (indirectly through the policy via engaging with reviews and providing submissions and evidence)
- Right to protection of families and children

6.2. Consideration of the Child Safe Standards and Universal Principle

The policy supports the Commission's commitment to safeguarding children and young people by embedding child-safe considerations into information security practices, systems and organisational culture:

1. Protection of children's personal and sensitive information
2. Risk-based approach to child safety and information security
3. Safe access to information and systems
4. Accountability, governance and oversight
5. Incident response and harm minimisation
6. Staff awareness and shared responsibility
7. Child-centred and culturally safe practices
8. Supporting participation and trust
9. Continuous improvement of child-safe capability.

This policy supports the Child Safe Standards and Universal Principle by ensuring that information security practices protect children's personal and sensitive information, promote strong governance and accountability, support safe participation, and reduce risks that could cause harm to children. Through risk-based controls, staff

awareness, and effective incident management, the Commission strengthens its capacity and culture to operate as a child-safe organisation.

6.3. Consideration of Reframing the Relationship commitments

This policy supports the Queensland Government's Reframing the Relationship commitments by embedding respect, accountability and shared responsibility for Aboriginal and Torres Strait Islander peoples into information security practices, governance and organisational culture.

This policy supports Reframing the Relationship commitments by ensuring that information security practices respect Aboriginal and Torres Strait Islander peoples, protect culturally sensitive information, support transparency and shared decision-making, and strengthen trust. Through strong governance, culturally capable practices and continuous improvement, the Commission reinforces its commitment to respectful partnerships and accountable public sector leadership.

6.4. Consideration of risk management

This policy supports the Commission's Risk Management Framework by identifying, managing and mitigating information security risks that may impact the achievement of organisational objectives, service delivery, compliance obligations and stakeholder trust.

This policy serves as a key control for mitigating information security risks identified in the Commission's Strategic and Operational Risk Registers by establishing clear requirements, responsibilities and governance arrangements for protecting information.

6.5. Consideration of privacy

This policy supports the Commission's obligations to manage personal information in a lawful, fair and responsible manner, and to protect the privacy of individuals whose information is collected, stored, used or disclosed by the Commission.

This policy supports effective privacy management by embedding information security controls that protect personal information, promote lawful and responsible information handling, and support transparency, accountability and public trust.

7. Supporting documents

Authority	Name
Framework or policy	QFCC Risk Management Framework
	Security Incident Reporting Policy
	Administrative Release of Information Policy
	Data Breach Policy
Procedures	Open data, information sharing, access and use procedure
	Data sharing guidelines (CSO)
	Data Breach Response Plan
	Record keeping Procedure
	Root Cause Analysis Procedure

Forms, templates and other supporting documents	Data breach reporting form

8. Definitions

Term	Definition
Agency	This refers generically to government and other statutory authorities (such as the Commission).
Authorised	Use individuals who have: • Received the appropriate authorisation (which must be signed and documented as stipulated in local business procedures) before operating the relevant device or service, • Agreed to abide by the policies, guidelines and local practice arrangements for use of the relevant device or service, and who have appropriately acknowledged this agreement where required.
Classification	The systemic arrangement of information into logical categories.
Employee	Those engaged on a permanent, temporary, seconded or contract basis. This also includes students, volunteers, work experience or other external persons and/or agencies.
Information	A collection of data in any form which is maintained by an agency or person, and which may be processed, analysed, interpreted, and stored by the information system. This information may be presented in electronic (digital), print audio, video, image, graphical, cartographic, physical sample, textual or numerical form.
Information Asset	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business function. Includes: paper-based records, digital records, information equipment, etc. ICT assets include all applications and technologies that are owned, procured and/or managed by an agency (i.e. desktop and productivity tools, application environments, hardware devices, systems software, management and control tools).
Information Owner(s)	The recognised officer(s) identified as having the authority and accountability under legislation, regulation or policy, for the collection and management of information assets on behalf of the Commission.
Information System Administrators	The recognised officer identified as managing and maintaining the configuration and reliable operation of an information system for the transmission, use and storage of information.
Information and Cyber Security Policy (IS18) (2025) based on ISO 27001.	Sets out the policy requirements for government departments and agencies when establishing, implementing and maintaining information security within their agency.
Information Systems	The organised collection of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.

Term	Definition
Queensland Government Enterprise Architecture (QGEA) framework	A decision-making and management framework that enables Queensland government departments and agencies to: collaboratively provide better and seamless services for Queenslanders; support more effective and efficient use of information and ICT in government; and support effective partnering with the private sector through the application of whole-of-Government, cross-agency and agency information and information communications technology policies and practices.
Queensland Government Information Security Classification Framework	A standard process that allows agencies to evaluate their information assets and to determine the appropriate level of security classification that must be applied to information assets as soon as possible after creation or receipt.
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Eligible data breach	A data breach involving unauthorised access to or unauthorised disclosure of personal information, or the loss of personal information in circumstances where unauthorised access or disclosure is likely, **and** where the access or disclosure is likely to result in serious harm to one or more affected individuals. Under the IP Act's MNDB scheme, agencies must assess suspected eligible data breaches and notify affected individuals and the OIC where serious harm is likely.

9. Document control

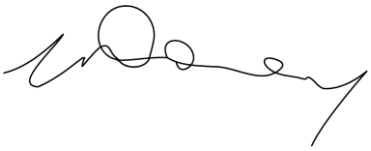
Document type	**Policy**	
Responsible Officer	Director Transformation, Governance and Change	
Content Manager references	PDF version:	D26/13689
	Word version:	D26/784
	Record of approval:	TF26/281 and TF26/1044
Information security classification	Official	
Document review	This policy is to be reviewed annually, or as required, in accordance with the Commission *Policy Framework*.	

9.1 Version control

Version	Date	Description of revisions	Author
2.0	April 2021	Most recent version	Unknown
3.0	July 2026	With new template and updated information to reference requirements of Mandatory Notifiable Data Breach Scheme	Manager Transformation, Governance and Change

10. Approval

Approval of operational policies is delegated to the Chief Operating Officer and the accountable officer.



Libby Doney
A/Chief Operating Officer
Queensland Family and Child Commission

5 August 2026