authority in the performance of its tasks.

Section 2 - Security of personal data

Article 32 - Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   a. the pseudonymisation and encryption of personal data;

   b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 - Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

   a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   b. communicate the name and contact details of the data protection officer or other contact point where more

Queensland Government Chief Information Office

(https://www.qgcio.qld.gov.au)

(https://www.qld.gov.au)

Information security policy (IS18:2018)

Policy

Final | June 2019 | v8.1.1 | OFFICIAL - Public | **QGCIO**

Purpose

The Queensland Government is responsible for a significant amount of information. To ensure trust and deliver business value it is critical that this information is protected appropriately.

This policy seeks to ensure all departments apply a consistent, risk-based approach, to the implementation of information security to maintain confidentiality, integrity and availability.

Policy statement

The Queensland Government will identify and manage risks to information, applications and technologies, through their life cycle, using Information Security Management Systems (ISMS).

Policy benefits

The implementation of this policy will:

- enable the Queensland Government to predict and respond to the changing threat environment
- enable Queensland Government to align to international best practice approaches
- facilitate a systematic approach to risk and improve decision making
- provide a flexible and tailored approach to meet individual department business needs and different risk appetites in an increasingly complex ICT and business environment
- allow for independent security system reviews to provide an increased level of confidence and trust in government
- support better allocation of time and resources to security challenges relevant to specific departments
- leverage increasing industry adoption of ISO 27001 which will assist in aligning requirements and improve transparency when using cloud and managed services.

Applicability

This policy applies to all Queensland Government departments (as defined by the Public Service Act 2008 (https://www.legislation.qld.gov.au/view/pdf/inforce/current/act-2008-038)). Accountable officers (not already in scope of the Public Service Act 2008) and statutory bodies under the Financial and Performance Management Standard 2019 (https://www.legislation.qld.gov.au/view/pdf/asmade/sl-2019-0182) must have regard to this policy in the context of internal controls, financial information management systems and risk management. Please see the Applicability of the QGEA (https://www.qgcio.qld.gov.au/information-on/qgea/applicability) for further information.

Policy requirements

Policy requirement 1: Departments must implement an ISMS based on ISO 27001

Departments must implement and operate an ISMS based on the current version of ISO 27001 Information technology - Security techniques - Information security management systems – Requirements (https://www.iso.org/isoiec-27001-information-security.html). The scope of the ISMS will include the protection of all information, application and technology assets.

Policy requirement 2: Departments must apply a systematic and repeatable approach to risk management

Risk management is an integral part of operating an ISMS where risks must be considered at a business level. Departments must adopt a risk management framework by integrating their ISMS into their corporate risk management processes.

Policy requirement 3: Departments must meet minimum security requirements

To ensure a consistent security posture and promote information sharing, Queensland Government departments must comply with the:

- Queensland Government Information Security Classification Framework (QGISCF) (https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf)
- Data encryption standard (https://www.qgcio.qld.gov.au/documents/data-encryption-standard)
- Queensland Government Authentication Framework (QGAF) (https://www.qgcio.qld.gov.au/documents/queensland-government-authentication-framework-qgaf)
- Australian Signals Directorate (ASD) “Essential Eight” Strategies (https://www.asd.gov.au/publications/protect/essential-eight-explained.htm)

Policy requirement 4: Departments accountable officers must obtain security assurance for systems

Every system is unique and security assurance should be applied sensibly and appropriately. Accountable officers must obtain security assurance to establish an understanding of information security protections and adherence to information security policy.

The level of security assurance applied to systems must be based on the criticality/significance of the system, using the business impact levels determination methodology outlined in the QGISCF.

See the Queensland Government information security assurance and classification guideline (https://www.qgcio.qld.gov.au/documents/information-security-assurance-and-classification-guideline) for more information.

Policy requirement 5: Accountable officers must attest to the appropriateness of departmental information security

Departmental accountable officers (CEO/Director-General or equivalent) must:

- endorse the Information security annual return (https://www.qgcio.qld.gov.au/documents/information-security-annual-return).
- attest to the department information security posture and compliance of its ISMS.

Endorsement must be obtained from the department's accountable officer through corporate audit and risk committee.

Departments should publish the attestation in a manner that is publicly accessible, for example:

- department website
- department annual report.

Issue and review

Version: v8.1.1
Issue date: 17 June 2019
Next review date: June 2020

This QGEA policy is published within the QGEA which is administered by the Queensland Government Chief Information Office. It was developed by the QGCIO Cyber-Security Unit and approved by the Queensland Government Chief Information Officer.

Implementation

This policy came into effect on **1 October 2018**.

Reporting requirements

This policy has specific reporting requirements:

#	Reporting requirement	Date
1	a) For the financial year ending 30 June 2019: • Departments must submit an Information security annual return that has been endorsed by the department's accountable officer to the Queensland Government Chief Information Office. • Departmental accountable officers must submit a letter of attestation to the Queensland Government Chief Information Officer.	30 October 2019

#	Reporting requirement	Date
	b) From 2020, for each financial year ending 30 June: • Departments must submit an Information security annual return that has been endorsed by the department's accountable officer to the Queensland Government Chief Information Office. • Departmental accountable officers must submit a letter of attestation to the Queensland Government Chief Information Officer	From 2020 annual at 30 September
2	Communicate incident response activities and threat intelligence to the Queensland Government Chief Information Office Virtual Response Team as per the QGEA Information security incident reporting standard. (https://www.qgcio.qld.gov.au/documents/information-security-incident-reporting-standard)	Ongoing

Last Reviewed: 26 September 2019