Information security policy

Version: 1.1 | **Version effective**: 12/05/2022

Audience

Department wide

Purpose

This policy supports the department's approach to managing information security in accordance with the Queensland Government's Information security policy (IS18:2018). This will enable the department to apply an Information Security Management System (ISMS) based on recommendations within ISO/IEC 27001 - Information technology – Security techniques – Information security management systems – Requirements (ISO 27001:2013).

Policy statement

The department will apply a consistent, risk-based approach to information security that maintains the confidentiality, integrity and availability of information by protecting information against unauthorised disclosure, access or use, loss or compromise (malicious or accidental), or a breach of privacy. This includes identifying and managing risks to information, applications and technologies, throughout their lifecycle by implementing an ISMS in compliance with the Queensland Government's Information security policy (IS18:2018).

Principles

- Departmental information (and/or data) is valuable and needs to be protected against the unauthorised disclosure, access or use, loss or compromise (malicious or accidental) or a breach of privacy that could have an adverse impact upon the department.
- A flexible and tailored approach to information security will meet business requirements, different risk appetites and levels of understanding of all employees. A consistent risk-based approach to information security reduces the likelihood and consequence of unauthorised disclosure, access or use, loss or compromise (malicious or accidental) or a breach of privacy to the department's information.
- The department proactively manages information risks by continual reviews and updates to procedures, processes, technical standards, and training materials as technology and threats change.
- Employees will be kept up-to-date with changes to information security requirements through departmental communication channels, updates to procedures and mandatory information security training.

- A systematic and repeatable approach to information security risk will improve decision-making, align requirements and improve transparency.

Requirements

- The department’s ISMS will be based on the current version of ISO/IEC 27001:2013.
- The ISMS uses the departmental Enterprise risk management framework to assess and understand the security risk for the department’s information. The department will ensure a consistent, cost effective and appropriate approach to the protection of information, information and communication technology (ICT) assets and facilities.
- Employees will manage and maintain the security of the information in their care by understanding their obligations under relevant departmental policies, legislation and guidelines including the Code of Conduct for the Queensland public service and departmental procedures, and by undertaking annual training.
- The department will ensure that their security position will be maintained through a continuous improvement cycle of assessments, reporting, risk management and assurances.
- The department will establish an internal strategic committee to oversee the department’s ISMS.
- The functions within the ISMS will be appropriately allocated with clearly defined roles and responsibilities.

Definitions

Term	Definition
Employee	Any permanent, temporary, seconded or contracted staff member, contractors and consultants, volunteers or other person who provides services on a paid or voluntary basis to the department that are required to comply with the department's policies and procedures. Within schools this includes Principals, Deputy Principals, heads of departments, head of curriculums, guidance officers, teachers and other school staff who manage information.
Data	The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not information until it is utilised in a particular context for a particular purpose.
ICT assets	ICT hardware, software, systems and services including voice, video and unified communication such as telephony and collaboration systems that are used in the department to process, store or transmit information such as computers, telephone systems, close circuit television (CCTV) and video surveillance systems, servers, switches, wireless network equipment, cabinets, scanners multifunctional printers, mobile phones, laptops, iPads, Surface Pros, digital cameras, electronic whiteboards, projectors etc.

Term	Definition
ICT facilities	An electronic service designed for a particular communication and/or function, which includes but is not limited to electronic networks, internet, extranet, email, instant messaging, webmail, fee-based web services and social media.
Information	Information is any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphic, cartographic, physical sample, textual or numerical form.
Information security	Information security is the preservation of confidentiality, integrity and availability of information, in addition to other properties such as authenticity, accountability, non-repudiation and reliability.
Information security management system (ISMS)	An ISMS is part of an overall management system (a type of framework), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
IS18:2018	Queensland Government's Information security policy (IS18:2018) issued by the Queensland Government's Chief Information Office (QGCIO) that directs agencies to implement an ISMS based on ISO/IEC 27001:2013, but does not require agencies to obtain ISO/IEC 27001:2013 certification.
ISO/IEC 27001:2013	ISO/IEC 27001:2013 is an international standard that provides a model for establishing, implementing, maintaining and continually improving an information security management system within an organisation. This international standard also includes requirements for assessing and treating information security risks tailored to the needs of the organisation. ISO/IEC 27001:2013 is enforced through QGCIO's Information security policy (IS18:2018).

Legislation

- Nil

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Information security procedure

Supporting information for this policy

- Nil

Other resources

- Queensland Government – Information security policy (IS18:2018)
- Enterprise risk management framework
- International Standard ISO 27001 - ISO/IEC 27001 - Information technology – Security techniques – Information security management systems – Requirements (ISO 27001:2013) website

Contact

For further information, please contact:

Information Management, Digital Technology
Information and Technologies Branch (I&T Branch)
Email: InformationManagement.INFOMNGT@qed.qld.gov.au

Cyber Security and Identity Management, Enterprise Technology Services
Information and Technologies Branch (I&T Branch)
Email: ISMS.GRC@qed.qld.gov.au

Review date

20/11/2023

Superseded versions

Previous seven years shown. Minor version updates not included.

Nil

Creative Commons licence

Attribution CC BY

Refer to the Creative Commons Australia site for further information