Information Security

Digital Policy
QH-POL-468:2019

1. Statement

Queensland Health maintains information security that enables modern healthcare delivery, using a risk-based and patient-centric approach to protect confidentiality, integrity and availability of information and information communication technology (ICT) assets, while protecting patients, staff and the organisation from real impacts.

2. Purpose

The purpose of this policy is to ensure Queensland Health protects its information against unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording, destruction, damage (malicious or accidental), fraud or a breach of privacy. This policy and its supporting standards enable a strong security culture, which will reduce risk and ensure all staff are meeting their responsibilities and duty of care as set out in the relevant Code of Conduct.

3. Scope

This policy applies to all Queensland Health employees, volunteers, contractors, consultants, working for:

- the Department of Health divisions, agencies and business units
- non-prescribed Hospital and Health Services
- prescribed Hospital and Health Services
- Managed Service Providers and their affiliates.

Note: Queensland Health Digital Policies define minimum requirements based on statutory obligations and risk. Development of local artefacts by Hospital and Health Services (HHSs) is only required where the policy or standard does not address local business needs.

The scope of this policy covers:

- all information in any format (physical, electronic or hybrid) that is created, collected, managed, stored and disseminated by Queensland Health to perform its business functions and deliver services to its customers. This includes clinical and non-clinical data such as patient, corporate, financial and workforce data
- all on-premise off-premises and cloud applications, systems and services
- Biomedical, Building Management System and specialty devices supported and connected to the Queensland Health network or a network maintained and supported by the Department of Health divisions, agencies and business units, HHS or other entity.

4. Principles

This policy is guided by the following information security principles:

- comply with applicable legislative and regulatory security requirements
- right information is accessed by the right people in the right place at the right time
- coordinate information security activities across Queensland Health
- manage information security risks effectively
- establish an effective information security culture
- regularly review and improve information security performance and capability
- provide health care practitioners an environment where the organisation can perform their work in a secure manner.

5. Information Security Objectives

The objectives are to:

- use a risk and privacy-based approach to protect confidentiality, integrity and availability of information assets and ICT assets
- implement a wholistic risk management approach to information assets and ICT assets, through systematically assessing, monitoring, and treating information security risks, and improving controls, while protecting patients, employees and organisations from real impacts
- define roles and responsibilities within Queensland Health and any third-party service providers.

6. Requirements

6.1 There is a Queensland Government requirement for Queensland Health to establish an Information Security Management System (ISMS) in line with the international standard ISO 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements*.

6.2 The Queensland Health ISMS contains the minimum requirements that all HHSs and the Department of Health must comply with.

6.3 Using the ISMS risk framework:

- each HHS must undertake a risk assessment to determine if the Queensland Health ISMS meets their business requirements and, where necessary, develop local policy artefacts to address any gaps identified
- all HHS and Department of Health staff must implement information security training commensurate with their risk appetite.

6.4 Each HHS must provide, accurate and comprehensive information to eHealth Queensland to enable Queensland Health to meet the mandated reporting requirements defined in the Queensland Government Enterprise Architecture ICT Profiling Standard.

6.5 Each HHS must report quarterly to the Cyber Security Group, eHealth Queensland, to ensure the Director General has state-wide oversight of information security risks, incidents and issues.

6.6 All actual security incidents or security vulnerabilities must be reported to the Cyber Security Group, eHealth Queensland; Anything rated High or Very High is to be reported immediately or within the timeframes stated in the Technical Vulnerability Management Standard and Information Security Incident Management Standard.

6.7 Queensland Health shall continually improve the suitability, adequacy and effectiveness of the ISMS.

7. Responsibilities

7.1 The Director-General, as System Manager, has overall accountability for information security, and ensuring Queensland Health complies with all applicable and relevant legal and regulatory requirements.

7.2 The Chief Executive, eHealth Queensland has overall responsibility for information security across the enterprise wide systems and applications supported and managed by eHealth Queensland.

7.3 The Chief Executive of Health Support Queensland (HSQ) has overall responsibility for information security across the enterprise wide systems and applications supported and managed by HSQ.

7.4 The HHS Chief Executive has overall responsibility for information security across HHS managed systems/all local systems in their HHS.

7.5 The Chief Information Security Officer, eHealth Queensland has responsibility for implementing

and maintaining the Queensland Health Cyber Security Strategy and Information Security Management System for Queensland Health.

7.6 The Information Security Committee (ISC) is responsible for setting the strategic direction and practices for information security to minimise threats and issues that impact Queensland Health to enable delivery of healthcare. The ISC has delegated accountability for managing information security matters across Queensland Health and to ensure compliance, efficiency and strategic alignment to minimise information security threats and issues.

7.7 Chief Officers, Executive Directors, Senior Directors, Directors and Managers are responsible for ensuring that the business areas for which they are responsible comply with this policy and the requirements set out in the supporting information security standards.

7.8 Application and Data Custodians (as defined in Queensland Health Data and Application custodianship – Roles & Responsibilities) are responsible for managing information security matters to ensure compliance with this policy and the requirements set out in the supporting information security standards.

7.9 All employees, contractors, agents and all persons with access to Queensland Health information assets have responsibility for diligently applying the requirements of this policy and the requirements set out in the supporting information security standards and relevant legislation.

8. Legislation and Supporting Documents

- *Crime and Misconduct Act 2001*
- *Criminal Code Act 1899*
- *Cybercrime Act 2001 (Cth)*
- *Information Privacy Act 2009*
- *Privacy Act 1990 (Cth)*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Right to Information Act 2009*
- Code of Conduct for the Queensland Public Service
- Department of Health Information Security Policy Framework
- Queensland Government ICT Profiling Standard
- Queensland Government Information Security Policy (IS18:2018)

9. Definitions

Term	Definition
Availability	A dimension in the assessment of the Technical Condition of an Application or Technology Asset in the Queensland Government. It measures absolute availability (the proportion of time a system is up and running, as compared to the time it is inoperable due to failures or scheduled maintenance).
Confidentiality	Ensuring that information is accessible only to those authorised and is protected from unauthorised disclosure or intelligible interception
Cyber Security	Cyber security is a key element of information security centred on the protection of information from unauthorised use or accidental modification, loss or release in internet connected systems.
ICT	Information and communication technology (ICT), also commonly referred to as Information Technology (IT) includes software, hardware, network, infrastructure, communications, devices and software systems (applications) that not only support business processes of an agency, but which enable the digital use and management of information and enable people to connect in a digital environment. Typically, ICT covers both the Application and Technology layers of the QGEA. Also see the Application and Technology QGEA classification framework domains for further examples.
ICT Asset	All applications and technologies that are owned, procured and/or managed by Queensland Health. These include desktop and productivity tools, application environments, hardware devices and systems software, network and computer accommodation, and management and control tools.
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, graphical, cartographic, physical sample, textual or numerical form. Information may also be a public record or an information asset if it meets certain criteria.
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 functions thereby satisfying a recognised agency requirement.
Information Security	Information security activities are concerned with the protection of information from unauthorised use or accidental modification, loss or release. Information security is based on three elements: • confidentiality – ensuring that information is only accessible to those with authorised access; • integrity – safeguarding the accuracy and completeness of information and processing methods; • availability – ensuring that authorised users have access to information when required.
Information Security Management System	Risk based approach controls framework as defined by ISO 27001:2013 Information technology – Security techniques – *Information security management systems – Requirements.*

Term	Definition
Integrity	A dimension in the assessment of Technical Condition for an Information Asset in the Queensland Government. It deals with the extent to which checks are implemented and enforced to ensure that an Information Asset remains true to its source.
Local System	System, software, devices procured and managed by the Hospital and Health services (HHS). Including any services provided via agreement between HHS and HHS.
Physical Asset	Includes but is not limited to information stored in a physical manner such as paper medical records, paper personal files, non-network connected laptops, and computers, mobile devices, recording devices, USB, back up tapes, cd's.
Physical Security	The means to provide physical protections of resources against deliberate or accidental threat.
Risk	The potential of an action or event to impact on the achievement of objectives.
Queensland Health	Queensland Health comprises of the Department of Health and the 16 independent Hospital and Health Services (HHSs). Queensland Health refers to the public healthcare sector, incorporating the Department of Health and HHSs. The Queensland healthcare system incorporates the public, private and not-for-profit healthcare sectors.

Version Control

Version	Date	Comments
1.0	30 July 2019	New policy