Information security

Policy

QH-POL-066:2014

1. Statement

The Department of Health maintains information assets and information communication technology (ICT) assets appropriately, lawfully and ethically using a risk-based approach to protect their confidentiality, integrity and availability.

2. Purpose

The intent of the Department of Health Information Security Policy is to:

- establish clear lines of accountability for information security
- embed information security into everyday practice by clarifying the actions required of all Department of Health staff to protect the Department of Health information assets and ICT assets appropriately
- identify, assess and manage information security risks at an acceptable level.

3. Scope

This policy applies to all employees, contractors and consultants within the Department of Health divisions and commercialised business units.

This policy can be used by Hospital and Health Services either as is, by re-branding or as a base for a Hospital and Health Service specific policy.

4. Principles

- **Risk-based** – information security decisions are made and recorded in accordance with Department of Health Integrated Risk Management Policy.
- **Accountable** - information security roles and responsibilities are clearly defined, communicated and acknowledged.
- **Appropriate** - access to and management of Department of Health information, information assets and ICT assets is appropriate and in accordance with the level of required security.
- **Addressed** – information security incidents are responded to promptly and appropriately, and longer term implications are addressed.
- **Integrated** – the information security considerations are incorporated into all areas of the Department of Health business.
- **Mature** - a mature information security culture is achieved via information security awareness.
- **Measured** – the performance of the information security policy and program of work is monitored, measured and reported.

5. Legislation

- *Cybercrime Legislation Amendment Act 2012 (Cth)*
- *Electronic Transactions Act 1999 (Cth)*
- *Evidence Act 1997*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Hospital and Health Boards Act 2011*

- *Information Privacy Act 2009*
- *Private Health Facilities Act 1999*
- *Public Health Act 2005*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*
- *Right to Information Act 2009*
- *Security Legislation Amendment (Terrorism) Act 2002 (Cth)*
- *Spam Act 2003 (Cth)*
- *Telecommunications Interception Act 2009*
- *Work Health and Safety Act 2011*
- *Work Health and Safety Regulation Act 2011*
- Queensland Government Enterprise Architecture, Department of Science, Information Technology and Innovation (DSITI):
  - Information Standard 18 - Information Security

6. Supporting documents

- Information Security Standard (available on Queensland Health intranet QHEPS)
- Information Security User Responsibilities Standard (available on Queensland Health intranet QHEPS)
- Storing Information on USB Drives Fact Sheet (available on Queensland Health intranet QHEPS)

7. Definitions

Term	Definition	Source
Availability	Ensuring that authorised users have access to information/equipment and services when and where required.	Queensland Government Chief Information Office (QGCIO) Glossary
Confidentiality	Ensuring that information is accessible only to those authorised and is protected from unauthorised disclosure or intelligible interception.	QGCIO Glossary
Domain	The categories used as part of the Queensland Government Enterprise Architecture (QGEA) to provide a consistent and convenient method of logically grouping business processes, information assets, applications and technologies and ICT initiatives into meaningful and manageable areas for analysis. For example, the Technology layer of the QGEA contains a domain for Desktop PCs.	QGCIO Glossary
Executive Officers	Divisional heads who directly report to the DoH Director-General.	Department of Health Definition
ICT	Acronym for Information and Communication Technology.	QGCIO Glossary
ICT Asset	All applications and technologies that are owned procured and/or managed by the Department of Health.	QGCIO Glossary
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	QGCIO Glossary

Term	Definition	Source
	knowledge in any medium or form.	
Information Asset	An information asset is 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. Examples of information assets include the Department of Health Annual Report, policies, statistical datasets, statistical publications, and applications (including the information held within) such as the Emergency Department Information System (EDIS), the Consumer Integrated Mental Health Application (CIMHA) and the Hospital Based Corporate Information System (HBCIS).	Department of Health Definition
Information Asset Custodian	The recognised officer responsible for implementing and maintaining an information asset according to the rules set by the owner – to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility throughout its lifecycle. The information asset custodian ensures a coordinated and documented approach to the quality assurance process of information asset management.	Department of Health Definition
Information Asset Owner	The recognised officer who is identified as having the authority and accountability under legislation, regulation or policy, for the collection and management of information assets on behalf of the State of Queensland, usually the Chief Executive Officer (CEO).	Queensland Government Chief Information Office Glossary
Information security incident	An identified occurrence or activity that has been successful in adversely affecting the security of information.	QGEA: Information Security Incident Management Guideline
Integrity	Safeguarding the accuracy and completeness of information and processing methods.	Department of Health Definition
Risk	An event that poses a negative threat (or potential positive opportunity) which might affect the course of the program or project.	QGCIO Glossary

Version Control

Version	Date	Comments
4.10	14 Feb. 2014	Finalised for approval.
4.11	21 May 2015	Transferred information to new template and reviewed by Information Security Unit.