ICT service continuity management

Department of Health Policy
QH-POL-457:2018

1. Statement

Information is a critical enabler for providing and improving health care as well as enabling the effectiveness of Queensland Health staff. Growing dependence on information and communications technology (ICT) and increasing integration between biomedical, imaging, management information and clinical systems supported by departmental and Hospital and Health Services (HHS) ICT service providers, demands higher system resilience, shorter recovery times and improved ICT continuity readiness to minimise impact on patient safety and clinical efficiency in the event of unplanned outages.

2. Purpose

This policy provides consistent, transparent and accountable governance processes and procedures to improve alignment of departmental ICT service continuity management (ICT SCM) with Queensland Health clinical and non-clinical functions that have critical ICT dependencies.

3. Scope

This policy applies to:

- all employees, contractors and consultants within departmental divisions and commercialised business units that are responsible for application and/or data custodianship and delivery of critical ICT services; and
- HHS and external ICT service providers who provide critical ICT applications, infrastructure and services to the Department of Health divisions and commercialised business units.

4. Principles

The department aligns its ICT service continuity approach to the principles of *International Standard ISO/IEC 27031*[1] and those required to establish and maintain an effective system of internal controls:

- **Accountability:** A single Application Custodian representing business criticality and continuity requirements on behalf of stakeholders provides linkage between HHS and/or departmental business continuity and ICT service continuity readiness. The Application Manager ensures the end-to-end redundancy, resilience and recovery performance of all component ICT systems supporting the application meets the agreed business criticality and continuity requirements.
- **Community of Practice:** Sharing knowledge and collateral between business stakeholders and ICT service provider teams enables continuous improvement and establishes a broader community of good practice.
- **Risk based approach:** Application of departmental risk management processes in line with levels of acceptable risk and risk appetite ensures consistent assessment of business criticality and consequent investment in ICT service continuity capability.
- **Managed:** Consistent practice, terminology and processes across ICT service provider teams enables better alignment, planning, coordination and validation of ICT service continuity readiness with HHS and departmental business continuity requirements. Consolidated reporting of ICT service continuity readiness for critical systems enables management of gaps and risks associated with misalignment of ICT service continuity with business expectations;

[1] Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity (2011)

- **Incident prevention:** Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attacks, and natural disasters, is critical to maintaining the desired levels of system availability for an organisation;
- **Incident detection:** Detecting incidents at the earliest opportunity will minimise the impact to services, reduce the recovery effort, and preserve the quality of service;
- **Response:** Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimise any downtime. Reacting poorly can result in a minor incident escalating into something more serious;
- **Recovery:** Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated later, or in some circumstances, not at all; and
- **Improvement:** Lessons learned from small and large incidents should be documented, analysed and reviewed. Understanding these lessons will allow the organisation to better prepare, control and avoid incidents and disruption;

5. Requirements

- ICT Service Continuity shall be managed in accordance with the requirements outlined in the Department of Health's ICT service continuity management standard.

6. Legislation

- *Hospital and Health Boards Act 2011*
- *Public Sector Ethics Act 1994*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Information Privacy Act 2009*

7. Supporting documents

- ICT Service Continuity Management Standard (QH-IMP-457)
- Emergency Preparedness and Continuity Management Policy (QH-POL-28028)
- Risk Management Policy (QH-POL-070:2015)
- Business Continuity Management Implementation Standard (QH-IMP-070-2:2017)
- Cyber Security Policy (QH-POL-066:2014)
- Information Security Standard (QH-IMP-066-1:2015)
- AS/NZS 5050:2010 Business continuity – Managing disruption related risk
- ISO 22301 Societal security – Business continuity management systems
- AS ISO 22301:2017 Societal security – Business continuity management systems - Requirements
- AS ISO 22301:2017 Societal security – Business continuity management systems - Guidance
- ISO 27031:2011 Information technology – Security and techniques – Guidelines for information and communication technology readiness for business continuity
- AS ISO/IEC 27035.2:2017 Information technology – Security techniques – Information security incident management
- AS ISO/IEC 27035:2017 Information technology – Security techniques – Information security incident management Guidelines to plan and prepare for incident response
- Data and Application custodianship – Roles and responsibilities (November 2017)

- ICT Critical and At-Risk Systems: Identification and Reporting Standard (QH-IMP-402-14:2018)

8. Definitions

Term	Definition
Application / ICT System	A software system deployed by the agency which has part of an agency's business process embedded with it.
Application Custodian	A position designated with accountability for the development, management, care and maintenance of an Application.
Application Manager	A position designated with responsibility for the day-to-day management of an application including the planning, development, installation, configuration, maintenance and support of the application.
Critical business functions / Critical processes	A business function, or part of a function (process), identified as time critical or essential for achievement of the department's objectives.
Critical ICT Service	An ICT system that is relied upon to the extent that an outage would pose significant risk to the business and therefore required a higher level of maintenance to ensure availability and performance. This is reflected in the ICT system having a consequence of failure of High or Very High according to the Department of Health risk analysis matrix. This would usually reference the business operation, delivery of safe clinical services, health service delivery or financial criteria.
Data Custodian	A position designated with responsibility and overall accountability for the Data within the Data Set, Data Collection and/or Application allocated and the capture, development, management, care and maintenance of the Data.
Hospital and Health Service (HHS)	A Hospital and Health Service established under Section 17 of the Hospital and Health Boards Act 2011.
ICT Service Continuity Management (ICT SCM)	The process, policies and procedures related to preparing for recovery or continuation of ICT infrastructure, systems and applications which are vital to an organisation after a disaster or outage. ICT Service Continuity focuses on the information, communication or technology systems that support business functions, as opposed to Business Continuity, which involves planning for keeping all aspects of a business functioning during disruptive events. ICTSC readiness enables good business continuity practice.
Queensland Health	Queensland Health comprises the Department of Health and sixteen independent Hospital and Health Services (HHSs). Queensland Health refers to the public healthcare sector, incorporating the Department of Health and HHSs.

Version Control

Version	Date	Comments
1.0	25/06/2018	New policy