**Policy Applies to:**

This policy applies to all employees of Mercy Hospital who have access to Mercy Hospital information systems and data networks.

Compliance with this policy for Contractors, Credentialed Specialists and Visitors engaged to work with, or who have access to Mercy Hospital information systems and data networks will be facilitated by Mercy Hospital Staff.

**Related Standard:**

- Standard 2.3 of the EQuIP programme.
- Privacy Legislation

**Rationale:**

This policy has been developed to provide a governing framework for Mercy Hospital's ICT systems, services and the information and data contained therein.

Technology-based systems are critical to the enablement of Mercy Hospital's business, clinical, and support operations. For the delivery of ICT systems and services (including the data produced and maintained within), it is necessary to ensure these are acquired, installed, maintained, and used in a safe, secure, and appropriate manner.

**Definitions:**

The terms used within this policy are defined in the ICT Definitions document
**See Appendix 1**

**Objectives:**

The objectives of this policy are:

- to provide a framework for the management of Mercy Hospital ICT Systems.
- to protect Mercy Hospital's ICT assets and the data that resides on the ICT systems.

It aims to address:

- **Integrity** – the appropriate maintenance, validation and protection of data and systems which includes the prevention of the unauthorised access, amendment, corruption or deletion of information.

- **Availability** – the appropriate access to systems and data to ensure that work or care is undertaken effectively and

- **Distribution** – the appropriate use of ICT systems and data throughout the organisation and to external sources which includes the prevention of the unauthorised distribution of information or resources.

- **To ensure business and patient Confidentiality** – the appropriate access to and use of data for the purpose of clinical care or business purposes including the

prevention of the inappropriate or unauthorised disclosure of information and protection of privacy

**STANDARDS**

All ICT Policies and Guidelines will be governed by this standard and by the over-arching objectives stated in this document

- Policies related to Privacy, Release of Information, Clinical Records Management are complied with and inform the principals of information management within the ICT policies
- Processes are in place to comply with appropriate operational and legislative requirements related to ICT
- Processes are in place to maintain Business Continuity and Disaster Recovery(DR/BC)
- Security processes are in place to ensure the integrity of confidential and sensitive information (refer to ICT Security Policy)
- Processes are in place to ensure that there is ICT support available from both Internal and/or External providers as required
- Mercy Hospital acknowledges that technological development and the use of ICT is advancing at a rapid pace and every attempt is made to keep up-to-date with safety and security within available resources.
- Mercy Hospital continually strives to implement latest versions of systems, and software applications, to ensure the integrity and safety of Hospital data.
- Validation of the integrity for Hospital data is undertaken periodically as appropriate
- Compliance with relevant national standards for Electronic Data Interchange (EDI) is met; including but not limited to: Ministry of Health, Primary care providers

**IMPLEMENTATION**

Education of all staff in the overview of ICT policies and guidelines will occur through mandatory training at induction and on an ongoing basis as required. All employees sign a Confidentiality Agreement and Email and Internet Use Standard at time of hire.
**See Appendix 2 and 3**

The ICT department provides support to all users who access the Hospital Systems and works closely with Third Parties and Vendors to ensure support for Clinical and Business units.

**EVALUATION**

Evaluation and monitoring is conducted by both Internal and External providers as is appropriate. Real-time system monitoring is in place to ensure integrity and safety of data and systems and can be accessed remotely by IT Department staff.

Evaluation takes place using a variety of methods including:

- Audits
- Incident forms

- Complaints
- System problem investigations
- Surveys

Refer to specific evaluation methods and processes related to individual ICT guidelines.

**Associated Documents**

- **External**
    - Privacy Act 1993
    - Health Information Privacy Code 1994
    - Relevant national ICT Strategy Standards
- **Internal**
    - Privacy/Release of Information
    - Clinical Records Management Policy
    - Information Management Policy
    - Information Communication Technology - Security Policy
    - ICT Guidelines-ICT Work Manual
    - Emergency Plan
    - Risk Management Policy
    - Social Media Policy