ICT SECURITY POLICY

Reviewed: July 2016

Policy Applies to:
This policy applies to all employees of Mercy Hospital who access 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 EQuIP5 programme.
Privacy Act 2003

Rationale:
This policy has been adopted as a means of protecting the confidentiality, integrity and access of Mercy Hospital's Information Computer Technology (ICT) systems, corporate and patient data.

Mercy Hospital's data is a valuable asset that must be afforded the highest level of protection for sensitive, confidential, commercial and/or privileged reasons.

Definitions:

The terms used within this policy are defined in the ICT Definitions document (**Appendix 1 of ICT Governance Policy)**

Implementation

Education of all staff will occur through mandatory training upon induction and on an as needed basis. Secure access is appropriate to Users specific roles undertaken in the organisation.

Process

a. The strategy for managing ICT security will be developed by the ICT team and approved by Mercy Hospital Executive.

b. ICT policies and guidelines will be available via Sharepoint, within the Mercy Policies tab
c. Violations of the ICT Security Policy may result in disciplinary action in accordance with Mercy Hospital Human Resource policies and procedures.

Exceptions to this Policy will be managed on a case by case basis by the ICT team and approved by Hospital Executive.

d. Throughout its lifecycle, all Mercy Hospital data shall be protected in a manner that is considered reasonable and appropriate to the level of sensitivity, value and criticality such data has to the Hospital.

e. Any Information System that stores, processes or transmits Mercy Hospital data shall be secured in a manner that is considered reasonable and appropriate to levels of sensitivity, value and criticality that data has to the Hospital.

f. Individuals, who are authorized to access Mercy Hospital ICT Systems, and the data contained therein, shall adhere to the appropriate roles and responsibilities granted to them, as defined in the ICT Policies.

Evaluation

Monitoring of the integrity of physical/environmental and software systems occurs both internally and externally by:

- CCTV is utilised to monitor specific entrances to the main building.
- Remote monitoring and reporting is available to the ICT staff through unique software applications that monitor and detect/alert device state, virtual capacity, hardware status, critical activity levels and failures.

Password protection guidelines and protocols are established to manage and monitor system access and use on an individual basis (Appendix 1).

Auditing of access to most systems is available through specific software applications.

Evaluation takes place using a variety of methods including:

- Audits
- Incident forms
- Complaints
- System problem investigations
- Surveys
- Adherence to Password protection guidelines

Associated Documents

- **External**
  - Privacy Act 1993
  - Health Information Privacy Code 1994
  - Relevant national ICT Strategy Standards

❖ 

Maintaining confidentiality

- **Internal**
  - Privacy/Release of Information Policy
  - Clinical Records Management Policy
  - Visitor Policy

- Information Management Policy
- ICT Governance Policy
- ICT Guidelines – ICT Work Manual
- Risk Management Policy
- Social Media Policy

❖ Mercy Hospital Human Resource policies and procedures.