Policy Applies to:

- All staff employed by Mercy Hospital.
- Contractors, credentialed specialists and allied health professionals who have access to Mercy Hospital information systems and data networks.

Related Standard:

Standard 2.3 of the EQuIP6 programme.
Health Information Security Framework (HISF) 2015
Privacy Act 1993.

Rationale:

Mercy Hospital's data is a valuable asset. Mercy Hospital is committed to protecting the confidentiality and integrity of corporate and patient data by utilising appropriate access controls across the Information Computer Technology (ICT) environment.

Objectives:

To exercise sufficient control over the Mercy Hospital ICT environment so that:

- Authorised users are able to access the systems and information required.
- Unauthorised users are prevented from accessing the environment.

Implementation:

Responsible Person

- The Information Communication Technology (ICT) Manager and his/her specified delegates will be responsible for implementation of the ICT Security Policy.

Data Security

- Confidentiality of information, including business, patient and staff identifiable information shall be protected in a manner reasonable and appropriate, at a minimum in accordance with relevant legislation/standards.
- Data shall be accessible to only those authorised to have access.

Physical Security

- Where practical, any office, ward area or support unit contain Mercy Hospital computer workstations shall be locked when left unoccupied.
- All Mercy Hospital workstations shall be locked (Ctrl + Alt + Delete) or logged off when left unattended.
- Personal computing and/or personal mobile devices may not be connected to the Mercy Hospital corporate network without prior approval from the ICT department.

Software Security

- Mercy Hospital deploy solutions on all workstations and servers to protect against malicious software. Users may not turn off or tamper with protection solutions (i.e. anti-virus).
- Users are not permitted to install software on Mercy Hospital computing equipment.
- As part of a regular maintenance cycle the ICT team will apply software patches to manage, remove or reduce security vulnerabilities.

Staff User Accounts

- Upon commencement of employment, all staff are assigned individual Mercy Hospital account credentials (username and password).
- Mercy Hospital user accounts will provide secure access appropriate to user's specific role(s) in the organisation.
- Education on good practice in selection, management and use of passwords will occur through staff orientation and on an as needed basis. For current password protection guidelines refer Appendix 1.
- Staff are responsible for all Mercy Hospital system access under their account credentials.
- Upon cessation of employment a staff member's Mercy Hospital user account will be deactivated.

Generic User Accounts

- Mercy Hospital generic user accounts facilitate access to shared workstations.
- Generic account access will be restricted to basic desktop functions, publically accessible information and documents relevant to all staff.

Support Accounts

- External support staff will be setup with temporary access rights restricted to the infrastructure and all applications they support.

Privileged Accounts

- Privileged access, (i.e. administrative privileges) will be provisioned via privileged accounts, separate from staff member individual user accounts.
- Privileged accounts will be used only for special activities requiring their use and not day-to-day activities.

Security Breaches

- Suspected ICT Security breaches, including inappropriate system access, should be reported to the ICT Team, ICT Manager or Mercy Hospital Executive.
- The impact of any security breach detected will be assessed by the ICT team and reported to the Mercy Hospital Executive.
- Violations of the ICT Security Policy may result in disciplinary action in accordance with Mercy Hospital Human Resource policies and procedures.

Remote Access

- Authorised staff, credentialed specialists, allied health professional and systems support contractors may be provisioned remote access to the Mercy Hospital ICT environment via a secured virtual private network (VPN).
- Remote access to the Mercy Hospital ICT network will be restricted to those resources required for an individual to fulfil their role(s).
- Remote access to the Mercy Hospital ICT environment may be subject to enhanced security controls, including multifactor authentication.
- All remote access attempts, both successful and unsuccessful, to the Mercy Hospital ICT environment will be logged and remain auditable for a period not less than 12 months.

Auditing & Monitoring

- Users should have no expectation of privacy with regards personal use of the corporate network, Mercy Hospital reserves the right to monitor any and all use of the computer network including review of emails sent/received, monitoring internet traffic and inspection of data stored on personal files.
- Mercy Hospital ICT systems will be capable of logging events that may have relevance to potential breaches of security.

Evaluation

Monitoring of the integrity of Mercy Hospital's ICT environment is supported by solutions that detect/alert device state, virtual capacity, hardware status, critical activity levels and failures. Enhanced monitoring solutions to detect abnormal behaviour within the ICT environment may reviewed by the ICT team.

Software applications that manage personally identifiable health information, or other data seemed sensitive, will support the auditing of record access. Audit may occur as result of a suspected security breach or privacy investigation.

Evaluation takes place using a variety of methods including:

- Ad-hoc security audits
- Incident forms
- Complaints
- Security breach investigation
- Adherence to Password protection guidelines
- Cyber security training programme and assessment

Associated Documents

- External
  - Privacy Act 1993
  - Health Information Privacy Code 1994
  - Health Information Security Framework (HISF) 2015

- Internal
  - Appendix 1 – Password Protection Guidelines
  - Privacy/Release of Information Policy
  - Information Management Policy
  - ICT Governance Policy
  - Risk Management Policy
  - Social Media Policy
  - Mercy Hospital Human Resource policies and procedures.