Policy Applies to:

This policy applies to all staff employed by Mercy Hospital. 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 EQuIP6 programme
Health Information Standards Organisation (HISO)
Health Information Security Framework (HISF)
ISO/IEC 38500:2015 Information Technology – Governance of IT for the organization
Privacy Act 2020
Ministry of Health – Digital, data and technology services – minimum requirements

Rationale:

Technology-based systems are a critical enabler of Mercy Hospital's business, clinical, and support operations. Appropriate levels of Information Communication Technology (ICT) Governance are necessary to promote the effective, efficient and acceptable use of ICT resources at Mercy Hospital.

Cultural Considerations:

Mercy Hospital recognise the importance of collecting, confirming, classifying, recording, storing and outputting data in a culturally appropriate manner. Specific considerations include:

- HISO Ethnicity Data Protocols (10001:2017)
- HISO Iwi Statistical Standards (10068:2017)

Where appropriate Mercy Hospital systems that manage patient and/or staff data shall support reporting across different Ethnicity Groups.

Definitions:

Authorised User: A member of Mercy Hospital staff or other individual who has been granted access to Mercy Hospital ICT systems for a specific purpose.

Information Communication Technology (ICT): Hardware, software, data and associated methodologies including but not limited to computers, computer systems, storage devices, cameras, mobile phones, telecommunications equipment, networks, databases and any other similar technologies as they come into use.

ICT Governance: Framework for leadership, organisation structures, business processes and standards which ensure that the organisation's ICT supports and enables achievement of its strategies and objectives.

Objectives:

The objectives of this policy are to promote effective, efficient and acceptable use of ICT in the organisation by:

- Outlining the system by which current and future use of ICT is directed and controlled.
- Providing a framework for the management of Mercy Hospital ICT Systems.
- Defining clear roles and responsibilities with regards the management of ICT.Ensuring Mercy Hospital's use of ICT systems conforms to relevant national health information standards.

IMPLEMENTATION

The principles by which ICT shall be governed, managed and operated are as follows:

Principle 1: Responsibility

- The ICT Manager, in collaboration with the Mercy Hospital Executive, is responsible for setting the strategic direction of Mercy Hospital's ICT investment in line with business needs.
- The Mercy Hospital Executive, in collaboration with Mercy Hospital governance and management committees, provide advice to the ICT Manager on priorities and emerging issues.
- The Mercy Hospital Clinical ICT Steering Committee identify, prioritise and monitor implementation of clinical technology initiatives.
- Project Sponsors are accountable for the delivery of individual ICT projects in accordance with the management methodology selected for the project.

Principle 2: Strategy

- The Information Communication Technology strategic plan identifies operational challenges and opportunities and outlines medium term priorities and technology roadmap.
- The strategic priorities and roadmap outlined in the ICT Strategic Plan are aligned to the targeted business strategies of the Mercy Hospital Tactical Framework.

Principle 3: Acquisition

- The acquisition of new ICT solutions aligns with the priorities outlined in the ICT Strategic Plan.
- The internal ICT department shall coordinate evaluation of new ICT solutions in collaboration with the impacted business users.
- The introduction of new ICT systems, both hardware and software, to the Mercy Hospital environment is coordinated through the internal ICT department. Mercy Hospital staff are not authorised to purchase and/or install technology solutions without prior approval.

- All proposals for ICT investment are to be considered and approved in accordance with Mercy Hospital financial delegations of authority and capital expenditure approval processes.
- A formal risk assessment using the GCIO Cloud Risk Assessment Tool is undertaken prior to implementation of a cloud based digital health solution.

Principle 4: Performance

- Processes and procedures are in place to ensure Mercy Hospital's ICT assets, both hardware and software, are managed, maintained, replaced and disposed of effectively.
- Security controls allow authorised users access to the Mercy Hospital ICT Environment while preventing unauthorised access, refer to ICT Security Policy.
- Tier 1 (basic help desk) and Tier2 (In-depth technical support) is provided to all authorised users of the Mercy Hospital ICT environment by the internal ICT department.
- Tier 3 (Expert product/service support) is coordinated by the internal ICT department and provided by external solution vendors as required.
- Software patches and/or upgrades recommended by solution vendors are applied in a timely fashion to ensure the integrity of Hospital data. Critical security patches are applied as soon as practical.
- Scheduled maintenance requiring a systems outage(s) shall be notified to impacted users at least 24 prior. Where practical outages are scheduled to minimise business impact.
- ICT risks are identified and adequately addresses in line with the Mercy Hospital Risk Management Framework. Adequate business resilience arrangements, including regular full system backups, are in place for disaster recovery.

Principle 5: Conformance

- Use of ICT systems will be consistent with relevant internal policies including Information Management, Privacy and Release of Information and Clinical Records Management.
- Use of ICT systems will be consistent with the minimum requirements for digital, data and technology services set out by the Ministry of Health.
- Processes and procedures are in place to comply with national standards with regards the management of health information including but not limited to those of the Health Information Standard Organisation (HISO) and the Health Information Security Framework (HISF).
- Compliance with relevant national standards for Electronic Data Interchange (EDI) are met.

Principle 6: Human Behaviour

- An overview of ICT policies and education on the acceptable user of Mercy Hospital's ICT environment occurs during new staff orientation and on an ongoing basis as required.
- All staff receive ICT systems training during orientation and on an ongoing basis as appropriate to their role.

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
- Post project reviews
- System problem investigations
- Surveys

Associated Documents

- External
    - Privacy Act 2020
    - Health Information Privacy Code 1994
    - Relevant national ICT Standards as above
- 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
    - Mercy Hospital ICT Strategic Plan
    - Mercy Hospital Tactical Framework.