TITLE:	**Cyber Security**		
Manual/Policy#:	MRHA Boards of Directors # III-7	**Entity:**	AGH/ CPDMH
Original Issue:	AGH: September 2019 CPDMH: May 2023	**Issued by:**	Allied Boards Chair and Allied Boards Secretary
Previous Date Reviewed:	AGH: September 2019 CPDMH: n/a	**Approved by:**	Allied Boards of Directors
Last Date Reviewed:	May 2023	**Cross Reference(s):**	MRHA Boards Policy #IV-8 Asset Protection, #II-2 Delegation of Authority and #III-3 Integrated Risk Management Framework

1. POLICY STATEMENT:

The Integrated President & Chief Executive Officer (CEO) is accountable to the Allied Boards of the Almonte General Hospital Corporation (including Fairview Manor and Lanark County Paramedic Service) and the Carleton Place & District Memorial Hospital Corporation ("the Corporations") to ensure that the Corporations and partners of the Corporations maintain adequate security over its data and information technology systems.

The Allied Boards role is to oversee the risk management process as it relates to cyber security.

2. SCOPE:

The Allied Boards is responsible for risk management and oversight as it relates to cyber security.

3. GUIDING PRINCIPLES:

Implementation of this policy will be guided by a proactive approach to mitigate risk from cyber breaches and or threats to ensure privacy and safety of health and business information and the threat of business interruption.

4. DEFINITIONS:

Cyber Security: Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

Incident Response - Incident response is a term used to describe the process by which the Corporations handle a data breach or cyberattack, including the way the corporations attempt to manage the consequences of the attack or breach. The goal is to effectively

manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as reputation, are kept at a minimum.

5. PROCEDURE:

The CEO will ensure that:

Training and Compliance

There is training and compliance plan for information technology/ cyber security throughout the Corporations by promoting a cultural awareness of cyber security and promote best practices as it relates to cyber security.

Risk Management Process

The Allied Boards through the Finance Resources and Audit Committee (FRAC) will oversee the risk management process through meeting on an annual basis to discuss policies, review key information assets and current vulnerabilities and set risk tolerance. (Reference: MRHA Boards Policy #III-3 Integrated Risk Management).

Incident Response Plan

The Allied Boards will review and approve the Incident Response Plan on an annual basis establishing its position in advance of a cyber security attack.

Cyber Security Insurance

The Corporations maintains adequate insurance. (Reference: MRHA Boards Policy #IV-8 Asset Protection)

Monitoring and Reporting

The CEO or delegate will provide the FRAC with a summary of information as it pertains to cyber security. The reporting will contain information from its partners as it relates to safeguarding of the shared electronic medical record and its hosted technology.

Offsite Service Providers

The CEO or delegate will ensure that offsite providers have a cyber plan in place and ensure that there is a monitoring system in place to provide reports. The CEO will ensure that due care is exercised in using offsite providers.

6. REFERENCES:

Imran Ahmad, Miller Thomson LLP, Cyber Security Readiness Measures Boards and Senior Leadership Teams Must have in Place, 2018.

7. **APPENDICES:** N/A

Evaluation: This policy will be reviewed every two years.