TITLE:	**Cyber Security**		
Manual/Policy#:	Board of Directors # III-7	**Division:**	AGH/ FVM/ LCPS
Original Issue:	September 2019	**Issued by:**	Board Chair and Board Secretary
Previous Date Reviewed:		**Approved by:**	Board of Directors
Last Date Reviewed:	September 2019	**Cross Reference(s):**	Asset Protection #IV-8, Delegation of Authority #II-2 Integrated Risk Management Framework #III-3

1. POLICY STATEMENT:

The President & Chief Executive Officer (CEO) is accountable to the Board to ensure that the Hospital and Hospital's partners maintain adequate security over its data and information technology systems.

The Board's role is to oversee the risk management process as it relates to cybersecurity.

2. SCOPE:

The Board of Almonte General Hospital is responsible for risk management and oversight as it relates to Cybersecurity.

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 an organization handles a data breach or cyberattack, including the way the organization attempts 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 President & CEO will ensure that:

Training and Compliance

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

Risk Management Process

The Board through the Finance and Audit Committee 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 Integrated Risk Management Policy Board of Directors #III-3)

Incident Response Plan

The Board will review and approve the Incident Response Plan on an annual basis establishing its position in advance of a cybersecurity attack.

Cyber Security Insurance

The Organization maintains adequate insurance. (reference Asset Protection Board of Directors #IV-8)

Monitoring and Reporting

The CEO or delegate will provide the Finance and Audit Committee with a summary of information as it pertains to cybersecurity. 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 annually.