MUSKOKA ALGONQUIN HEALTHCARE		**Policy/Procedure Name:**	**Information Security**
Manual:	ICT	**Number:**	N/A
Section:	N/A	**Effective Date:**	DD MMM YYYY
Pages:	1 of 9	**Revision Date:**	DD MMM YYYY

Purpose

This information security policy is designed to support the Muskoka Algonquin Healthcare (MAHC) strategic plan and forms the basis of the Information Security Management System (ISMS) framework.

Scope

This policy applies globally to all people, processes and assets.

Policy Statement

The objectives, for the Muskoka Algonquin Healthcare (MAHC) ISMS framework, are:

- To uphold MAHC' mission, vision, values and objectives by protecting MAHC' information assets for confidentiality, integrity and availability;
- To ensure that MAHC can continue to provide quality health care services in the event of information security incidents;
- To sustain MAHC' strategic plan by strengthening key organizational enablers with good security practices – including the protection of sensitive patient information.

The objective for MAHC' information system policy is established and maintained by the IM/IT Steering Committee. MAHC IM/IT Steering Committee is responsible for overseeing and annually reviewing the information security policy objectives to ensure that they remain practical and in line with MAHC strategic directions and goals.

The Chief Financial Officer, Corporate Services and Risk is responsible to approve objectives set by the MAHC IM/IT Steering Committee

Definitions

Accountability

Assuring that users are accountable for their actions. This includes auditing capabilities which can be used to track actions, detect intrusions or reconstruct events.

Asset

Any data, device, system, other components of the environment or resource that supports information-related activities and provides value to the organization. Some examples of assets are hardware, software, services, facilities and confidential information.

Asset Owner
Person or group identified by management as being ultimately responsible for the maintenance of the confidentiality, integrity and availability of an asset.

Availability
The asset is available when it is needed. This includes the correct functioning of computing systems used to store and process information, security controls used to protect the asset and the communication channels used to access the asset.

Confidentiality
The assurance that information is not disclosed to unauthorized recipients. This includes classifying information and ensuring the appropriate restricts are applied according to its classification.

External Party User
A person from a party, external to the organization, which is granted access to organization assets. This includes customers, contractors, service providers, suppliers and volunteers.

Information Security
The practice of protecting the confidentiality, integrity and availability information assets.

HIC
Health Information Custodians

Information Security Event
A negative occurrence that can be observed, verified or documented that affects the confidentiality, integrity and availability of organization assets.

Information Security Incident
A series of information security events that negatively affect the organization and/or impact its security posture.

Information Security Incident Management
The monitoring and detection of information security incidents and events and the execution of proper responses to those incidents and events.

Information Security Policy
Highest level ISMS policy, which has management approval and sets the organization approach for managing information security objectives.

Information Security Management System (ISMS)
A set of policies concerned with information security management and information technology-related risk designed with the objective to support the organization's strategic plan. This includes the information security policy.

Information Technology (IT)
The application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

Integrity

The accuracy and consistency of asset data is maintained and assured over its life-cycle. This includes protecting data from unauthorized or undetected modification.

Malware

Software designed to exploit, infiltrate or damage a system without the informed consent of the system. This includes computer viruses, worms, Trojans, rootkits, spyware, adware and other malicious software.

Patients

Patients and communities served by Grey Bruce Health Services.

Principle of Least Privileged

The principle states that the least amount of access and permissions are granted for a user to be able to perform his role and responsibilities.

Risk

The potential impact and probability of an event that can compromise organization assets.

Risk Assessment

The overall process of analyzing and evaluating risk. This includes maintaining information security risk criteria; applying consistent and valid risk assessment methodologies, and identifying risks.

Risk Management

The overall process of managing risk which is composed of risk assessment and risk treatment.

Risk Treatment

The process of selecting and implementing measures to handle identified risk. This includes accounting for the risk assessment results and formulating security risks treatment plans.

User

Anyone who is granted access to organization assets. This includes organization employees and external party users.

Shall/Must

Used for absolute requirements, they are not optional.

Should

When valid reasons exist within certain circumstances not to implement a requirement, however; the implications must be understood and consideration on implementation of compensating control/s must be performed.

May

The requirement is only a recommendation or has been provided as an implementation example and is not intended on being exhaustive.

Procedure

Though specific roles and responsibilities for ISMS are outlined in this section of the policy, it is important to note that information security is the collaborative responsibility of everyone at GBIN. Any information security incidents or weaknesses must be reported to the [A3: title of individual].

A1: title of individuals or group: are responsible for:

(a) Overseeing and annually reviewing the information security objectives;
(b) Approving this policy.

Comment [A1]: e.g. CISO? CIO? CSO?

Comment [A2]: Who?
e.g. **Executive Team? Board of Directors?**

A3: title of individual: is responsible for:

(a) Establishing and maintaining the objectives of this policy;
(b) Reviewing the ISMS at least once a year, and each time a significant change occurs, to ensure that the ISMS suitably, adequately and effectively supports the corporate information security objectives. Meeting minutes of these reviews must be kept.
(c) Ensuring that the ISMS is implemented according to this policy, for the protection of assets, and for the success of the information security program. This includes ensuring the proper communication of this policy.
(d) Understanding and mitigation of information security risks. This includes operational coordination and maintenance of the ISMS to ensure that healthcare services are not disrupted due to security issues.
(e) Reporting to the President and Chief Executive Officer, as soon as possible, any possible breach of this policy and its impact on the organization.

Comment [A3]: e.g. CISO? CIO? CSO?

President and Chief Executive Officer: is responsible for:

(a) Ensuring sufficient support of this policy – this includes adequate resourcing for information security;
(b) Ensuring sufficient support for the **A3: title of individual** in the maintaining of information security – including ensuring sufficient authority is granted to the **A3: title of individual** to carry out his responsibilities.

Comment [A4]: e.g CISO? CIO? CSO?

Comment [A5]: e.g CISO? CIO? CSO?

Ultimate Designated Person: is responsible for:

(a) Ensuring that this document is managed and maintained up-to-date;
(b) Ensuring the proper communication of this policy.

A4: title of individual: is responsible for:

(a) Ensuring that the appropriate human resource security is in place prior to, during, and at termination and change of employment of employees. This includes ensuring that the appropriate information security awareness, education and training is in place for employees.

Comment [A6]: e.g CISO? CIO? CSO?

Comment [A7]: **Vice President, People & Organizational Effectiveness, Chief Human Resources Officer?**

Asset Owners: are responsible for:

(a) Maintaining the confidentiality, integrity and availability of asset(s) under their responsibility and must uphold the principles of this policy and any other applicable security policies, standards and supporting documents.

1 Policy Principles

These principles serve as a foundation to support a common policy framework, listed below are the guiding principles of the various policies in support of an ISMS policy framework.

1.1 Acceptable Use of Information and Information Technology

- GBIN must define behavioral requirements governing the acceptable use of information and information technology to which GBIN information systems, agents and Electronic Service Providers, must adhere to.

Refer to the Acceptable Use of Information and Information Technology Policy.

1.2 Information Security Training

- GBIN must foster an information security-positive culture. This may be achieved by implementing an information security awareness and education program to help all persons with access to The GBIN to understand their information security-related obligations.

Refer to the Privacy and Security Training Policy.

1.3 Threat Risk Management

- GBIN must perform information security threat risk assessments (TRAs) and must track, and mitigate or formally accept all the risks that are identified through a TRA.

Refer to the Threat Risk Management Policy.

1.4 Cryptography

- GBIN must implement cryptographic solutions to protect the confidentiality and integrity of PHI where appropriate, as well as to confirm the identity of the originator of a communication.

Refer to the Cryptography Policy.

1.5 Information and Asset Management

- GBIN must classify and define protection requirements for PHI in The GBIN in a manner that protects its confidentiality, integrity, and availability in any from (e.g., paper or electronic) throughout its information lifecycle.

Refer to the Information and Asset Management Policy.

1.6 Access Control and Identity Management

GBIN must establish appropriate access and identity management controls to manage all persons and information system access, these controls must:

- Define the information security responsibilities of all persons who have access to GBIN information systems
- Ensure that only authorized persons are granted access and that personal accountability is assured
- Ensure that only authorized information systems are granted access and provide authorized persons or information systems with only the least amount of privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Refer to the Access Control and Identity Management Policy.

1.7 Logging and Monitoring

- GBIN must log and monitor all access to information systems, and must log and monitor information system events.

Refer to the Security Logging and Monitoring Policy.

1.8 Network and Operations

- GBIN must implement controls to secure their network infrastructure, and establish procedures to secure the ongoing management and operation of GBIN information systems.

Refer to the Network and Operations Policy.

1.9 System Development Lifecycle

- GBIN must define information system development and change control requirements, and ensure that all system development activities performed are carried out in accordance with these requirements.

Refer to the System Development Lifecycle Policy.

1.10 Electronic Service Providers

- GBIN must ensure that their Electronic Service Providers who will have access to GBIN information systems, or who manage or provide support have adequate information security controls in place to protect and maintain the level of confidentiality, integrity and availability.

Refer to the Electronic Service Provider Policy.

1.11 Physical Security

- GBIN must implement controls to protect against the risks of unauthorized physical access and environmental damage to information systems, identity provider services and data contribution endpoints.

Refer to the Physical Security Policy.

1.12 Business Continuity

GBIN must implement procedures necessary to ensure that information systems:

- Remain available, especially in the event of a disaster, or
- Can be recovered if operations are disrupted.

Refer to the Business Continuity Policy.

1.13 Information Security Incident Management

- GBIN must implement an information security incident management process to identify and resolve information security incidents related to information systems quickly and effectively, while minimizing their impact and reducing the risk of similar information security incidents from occurring.

Refer to the Information Security Incident Management Policy.

1.14 Privacy and Security Assurance

- GBIN must identify and mitigate privacy and security risks and areas of non-compliance in respect of GBIN information systems, through privacy impact assessments, threat risk assessments, privacy and security readiness self-assessments, privacy and security operational self-attestations, auditing and monitoring activities and assurance of agents, Electronic Service Providers and third parties.

Refer to the Privacy and Security Harmonized Assurance Policy.

Cross Reference

N/A

Notes

This material has been prepared solely for the use at Muskoka Algonquin Healthcare. Muskoka Algonquin Healthcare accepts no responsibility for the use of this material by any person or organization not associated with Muskoka Algonquin Healthcare. No part of this document may be reproduced in any form for publication without permission of Muskoka Algonquin Healthcare.

References / Relevant Legislation

Documents that are referenced in, or support, this corporate information security policy and the information security management framework:

- Acceptable Use Policy;
- Privacy and Security Training Policy
- Threat Risk Management Policy
- Cryptography Policy
- Information and Asset Management Policy
- Access Control Policy;
- Security and Logging and Monitoring Policy;
- Network Operations Policy
- Electronic Service Providers Policy <- May not be applicable or combined into another policy
- System Development Lifecycle Policy
- Physical Security Policy;
- Business Continuity Policy
- Information Security Incident Management Policy
- Privacy and Security Harmonized Assurance Policy <- May not be applicable or combined into another policy

Appendices

N/A