1.0 Policy:

It is Sunnybrook's policy to protect the hospital's information assets from all security threats, whether internal or external, deliberate or accidental.

2.0 Overview

Protection of Sunnybrook's information assets, including the technology resources that support the hospital enterprise, is critical to the functioning of the hospital.

Information assets, including the personal health information of our patients, are at **risk** from potential threats such as employee error, malicious or criminal action, information management system failures, and natural disasters. These types of threats could result in the loss of the **confidentiality, availability or integrity** of Sunnybrook's information systems, services or data resources, including but not limited to: damage to or loss of information assets; corruption or loss of data accuracy or reliability; interruption of the administrative and clinical activities of the hospital; compromise in the confidentiality of personal health information or the privacy rights of patients.

In order to manage the risks presented by potential threats to our information assets, Sunnybrook maintains an **Information Security Management System (ISMS)** which includes this **Information Security Policy**, as well as technical and administrative controls appropriate for the protection of these assets as documented in the **Information Security Standards of Practice**. The ISMS is intended to enable Sunnybrook management to establish, implement, operate, monitor, review, maintain and improve hospital information security. Sunnybrook's Chief Security Officer is accountable for the performance of the ISMS.

3.0 Applicability

This policy applies to all Sunnybrook employees, medical staff, students, volunteers, members, officers, directors, researchers, instructors, agents, vendors, contractors, consultants and related entities including such Foundations, Research Institutions and others, whether individual or corporate, (each of which individually and collectively are included within the meaning of the term "Sunnybrook") and any external parties who, under contractual obligation, on behalf of or for the purposes or benefit of Sunnybrook, may come into contact with Sunnybrook information assets.

4.0 Procedures:

Sunnybrook operates in accordance with and maintains **Security Standards of Practice** which are corporate confidential. Questions regarding internal standards of practice should be directed to Sunnybrook's Chief Privacy Officer at (416) 480-6100 x3538 or privacy@sunnybrook.ca .

5.0 Information Security Requirements

5.1 Security Requirements Framework

Sunnybrook's Security Framework addresses the following general requirements for information security based on generally accepted security standards applied within a healthcare delivery context:

- **Risk Assessment, Sensitivity and Criticality** – requires a defined taxonomy of the *sensitivity* of electronic information resources and the *criticality* of information resources, to be used for assessing risk, incident response planning, and notification in instances of security breaches.

- **Logical Security** - security measures for controlling access to electronic information resources through *logical* means (e.g., via software or network controls), procedural controls related to secure software development and change control, security of data in motion and at rest (including encryption controls), communications security, and reduction of risk from intrusive and malicious computer software acting on vulnerable corporate systems.

- **Physical Security** - security measures for controlling physical threats and access to electronic information resources through physical means, including environmental and disaster prevention and recovery controls, physical location and equipment access controls, device and media controls, and procedural controls over financial and administrative assets and instruments (e.g. check stock and maintenance records).

- **Disaster Recovery and Emergency Procedures** – requires a description of requirements for Disaster Recovery Plans and emergency procedures.

- **Managerial Security Measures** - security measures with respect to employment and other organizational matters, actions to be taken with respect to suspected violations of these Guidelines, and workforce security and awareness training.

- **Security Program Responsibilities** – governance, management and operational responsibilities for maintenance and implementation of the Sunnybrook Security Program and the controls outlined in this Policy.

5.1.1 Applicability of the ISO 27002 Standard to the Sunnybrook Privacy and Security Framework

The ISO/IEC 27002 standard is a widely adopted international standard for initiating, implementing, maintaining, and improving information security management in an organization. Sunnybrook has, in conjunction with other applicable standards including Canadian legal requirements, **adopted the ISO 27002 standard as a reasonable framework for identifying requirements for and implementing security controls.** ISO 27002 indicates why security is needed, how to assess security control requirements, and provides guidance on how to assess risks to information assets and how to assign specific controls. The 27002 standard is organized into ten sections, each covering a key control area for information security:

The ISO/IEC 27002 standards supports the essential framework for establishing information security controls within the context of the ISO 27001 standard for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an **Information Security Management System** (ISMS). The ISMS provides Sunnybrook management with a 'planning and management' model for an overall **Information Security Program** and is documented separately.

Sunnybrook's security procedures follow the format of the ISO 27002 standard and references all 12 security control objectives found in that standard.

2.1.2 Applicability of Other Standards Affecting or Requiring Information Security Assurance

PCI DSS v3.0

Sunnybrook is committed to designing and maintaining corporate governance practices that are consistent with applicable regulatory and contractual requirements, responsibilities and obligations related to the **Payment Card Industry (PCI) Data Security Standard (DSS)[1].** The PCI DSS is a worldwide standard endorsed by all major credit card brands, designed and maintained by The PCI Security Standards Council (SSC), and intended to protect cardholder data wherever it is processed, stored or transmitted.

Currently, Sunnybrook is considered a 'Level 4 merchant' as per Visa and manages multiple payment card systems at point of sale throughout Sunnybrook facilities. Sunnybrook is required by contract with our payment card service provider to comply with the PCI DSS v3.0 standard in operation of the payment card services.

The following table indicates the requirements of the PCI DSS standard which have been reviewed and incorporated into this security policy to reflect Sunnybrook's obligations therein. References to specific PCI DSS sub-requirements that have been incorporated throughout this policy are indicated below:

Security Domain	PCI Requirements
Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12. Maintain a policy that addresses information security for all personnel.** This security policy will be inclusive of, but not limited to, the following requirements in support of PCI DSS Requirement 12:

[1] https://www.pcisecuritystandards.org/security_standards/

	PCI DSS Section 12.1.3: Annual policy review and updates to policy when the environment changes. PCI DSS Section 12.3: Establish appropriate usage policies for critical employee-facing technologies PCI DSS Section 12.4: Security policy and procedures will clearly define information security responsibilities for all personnel. PCI DSS Section 12.5: Assign to an individual or team the information security management responsibilities. PCI DSS Section 12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. PCI DSS Section 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.

Canada Health Infoway Consumer Health Application Certification Requirements

Sunnybrook operates a *personal health record* (PHR) service for our patients and on behalf of our community partners and their patients called "MyChart"[2]. Sunnybrook intends to maintain Canada Health Infoway Consumer Health Application Category 3 Certification[3] for MyChart which requires that the scope and operations of Sunnybrook's information security program include MyChart information assets and service operations and also requires attestation to specific control elements of the security program that are intended to support MyChart.

As noted elsewhere in this policy, Sunnybrook has designed its security program to adhere to generally accepted standards for security assurance and has explicitly based our security program on one or more standards recognized by CHI which they also employ for certification purposes, including the Canada Health Infoway Electronic Health Record Infostructure (EHRi) Privacy & Security Conceptual Architecture, The International Organization for Standardization's Code of Practice for Information Security Management - ISO 17799:2005; ISO 27001 - Information Security Management Systems Requirements; ISO 27002 - Code of Practice for Information Security Management; ISO 27799:2008 - Information Security Management In Health[4].

The following table references control elements of Sunnybrook's security program that are intended to be applicable to MyChart assets and service operations:

Control category	**Policy Reference**
User Identity Management	2.9.2 – User Management and Section 4.6 - Personnel Security

[2] http://sunnybrook.ca/content/?page=mychartlogin-learnmore

3 A consumer health application is an electronic solution that enables the consumer to collect, retrieve, manage, use and share personal information and other health-related data. See https://www.infoway-inforoute.ca/en/component/content/article?id=236

[4] https://www.infoway-inforoute.ca/en/our-partners/vendors/certification-faqs

Access Control	2.9.1 - Business requirement for access control
Data Integrity	2.2.2 - Electronic Information Resource Sensitivity 2.4.2 - Security of third party access 2.4.3 - Outsourcing 2.8.1 - Incident management procedures 2.8.4 - Housekeeping 2.8.7.6 - Publicly available systems 2.8.8 - Protection against malicious software 2.10.3 - Cryptographic controls 2.10.4 - Security of system files
Data Availability	2.2.3 - Electronic Information Resource Criticality 2.4.3 - Outsourcing 2.8.4 - System planning and acceptance 2.8.4 - Housekeeping 2.11 - Incident Management
Audit	2.4.2 Security of third party access 2.4.3 – Outsourcing 2.6.1.3 - Confidentiality Agreements 2.7.1.2 - Physical entry controls 2.8.1 - Operational procedures and responsibilities 2.8.1.2 - Operational change control 2.8.1.3 - Incident management procedures 2.8.6.1 - Management of removable computer media 2.8.6.2 - Disposal of media 2.10.2 - Security in application systems – (Audit) 2.11 - Incident Management
Logging	2.8.4.2 Operator logs 2.8.4.3 Fault logging 2.9.7 Monitoring system access and use 4.9.7.1 Event logging 4.9.7.2 Monitoring system use 4.9.7.3 Clock synchronization
Data Confidentiality	2.2.2 - Electronic Information Resource Sensitivity 2.4.2 - Security of third party access 2.4.2.4 - Security requirements in third party contracts 2.4.3 – Outsourcing 5.5 - Information Asset Identification, Classification and Ownership 2.6.1.3 - Personnel Security- Confidentiality Agreements 2.8.1.1 - Documented operating procedures 2.8.1.3 - Incident management procedures 2.8.7.4.2 - Policy on electronic mail 2.9.2.3 - User password management 2.9.3 - User responsibilities 2.10.3 - Cryptographic controls