Team Name: Information and Communication Technology Team Lead: Regional Director of Information and Communication Technology Approved by: VP - Corporate Services	Reference Number: ORG.1610.PL.001 Program Area: Information and Communication Technology Policy Section: General
Issue Date: April 15 2019 Review Date: Revision Date:	Subject: Information and Communication Technology (ICT) Security

POLICY SUBJECT:

Information and Communication Technology (ICT) Security

PURPOSE:

Southern Health-Santé Sud is committed to fulfilling its business objectives and supporting the mandate of Manitoba eHealth to assure the continued delivery of services by safeguarding Information and Communication Technology (ICT) Assets.

Southern Health-Santé Sud has designated the responsibility to design and implement security safeguards related to ICT Assets to the Southern Health-Santé Sud's ICT department.

The purpose of this policy is:

- To provide specific direction for the safeguarding of ICT Assets;
- To reduce organizational risk associated with unsecure ICT Assets; and
- To preserve confidentiality, integrity and availability of ICT Assets and enforce accountability for the use of ICT Assets

BOARD POLICY REFERENCE:

Executive Limitation 1: Global Executive Restraint & Risk Management

Executive Limitation 7: Corporate Risk

POLICY

Roles and Responsibilities:

- Southern Health-Santé Sud Chief Executive Officer (CEO) – The CEO is accountable for the safeguarding of ICT Assets and acceptance of ICT security risk within Southern Health-Santé Sud. The CEO is responsible for designating an Information Security Officer (ISO) for Southern Health-Santé Sud.
- The Manitoba eHealth Chief Information Officer (CIO) – The CIO is responsible for the management of programs for safeguarding of ICT Assets and identification of ICT

security risk on behalf of Southern Health-Santé Sud. The CIO will inform the CEO of Southern Health-Santé Sud on all significant ICT security matters.

- The Southern Health-Santé Sud Information Security Officer (ISO) - The ISO is accountable to the CEO for ensuring the following specific responsibilities are met:
  - The effective and efficient management of an ICT security program developed by Manitoba eHealth;
  - Day to day secure operations of Southern Health-Santé Sud application services;
  - Development, implementation and monitoring of standards, processes, and practices as they relate to security, based on industry best practice;
  - Maintaining the security direction of the enterprise architecture.
  - Ensuring security policies, procedures, and standards are adhered to.
  - Providing basic security support for all systems and users.
  - Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
  - Educating Custodian and User Management with comprehensive information about security controls affecting system Users and application systems.
  - Providing on-going employee security education and awareness.
  - Performing security audits.
  - Reporting regularly to the Manitoba eHealth CIO and the Southern Health-Santé Sud Senior Management Team in regards to the status of information and communication technology security.
- Business Owner – Responsibilities include:
  - Knowing the information for which she/he is responsible.
  - Assisting to determine a data retention period for the information, with consideration of any legislative requirements.
  - Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
  - Authorizing access and assigning custodianship.
  - Specifying controls and communicating the control requirements to the Custodian and Users of the information.
  - Reporting immediately the loss or misuse of Southern Health-Santé Sud information and unauthorized disclosures of PHI promptly to the Privacy Officer following Southern Health-Santé Sud procedures.
  - Initiating corrective actions when problems are identified.
  - Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
  - Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.
- The Custodian - Responsibilities include:

- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.
- Providing access to information as authorized by the Business Owner and the Privacy Officer for use and disclosure using procedures that protect the privacy of the information.
- Evaluating the cost effectiveness of controls.
- Adherence to information security policies, standards and procedures.
- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- Reporting immediately the loss or misuse of Southern Health-Santé Sud information and unauthorized disclosures of PHI promptly to the Privacy Officer following Southern Health-Santé Sud procedures.
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

➢ User Managers: User Managers are responsible for overseeing their employees' use of Information Systems, including:
- Ensuring that information is only accessed in support of authorized job responsibilities, and limited to the minimum amount necessary.
- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- Ensuring compliance with Information Security Policies and Standards and with all controls established by the Business Owner and Custodian.
- Reporting immediately the loss or misuse of Southern Health-Santé Sud information and unauthorized disclosures of PHI promptly to the applicable Privacy Officer, following Southern Health-Santé Sud procedures.
- Monitor employees to ensure they keep personal authentication methods (e.g. passwords, SecureCards, PINs, etc.) confidential.
- Initiate corrective actions when problems are identified.

➢ User: A User of information is expected to:
- Access information only in support of their authorized job responsibilities.
- Comply with Information Security Policies and Standards and with all controls established by the Business Owner and Custodian.
- Report immediately the loss or misuse of Southern Health-Santé Sud information and unauthorized disclosures of PHI, promptly to the immediate supervisor, following Southern Health-Santé Sud procedures.
- Keep personal authentication methods (e.g. passwords, SecureCards, PINs, etc.) confidential.
- Report problems and participate in corrective action.

Computer and Information Control

All systems and information are assets of Southern Health-Santé Sud and protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

- Software
  - Software Ownership: All computer software developed by Southern Health-Santé Sud employees or contract personnel on behalf of Southern Health-Santé Sud or licensed for Southern Health-Santé Sud use is the property of Southern Health-Santé Sud and must not be copied for use at home or any other location, unless specified by the license agreement.
  - Software licensing: All software packages that reside on computers and networks within the Southern Health-Santé Sud must comply with applicable licensing agreements and restrictions, with Southern Health-Santé Sud acquisition of software policies
  - Software usage: All software installed on computers and networks within the Southern Health-Santé Sud must first meet established guidelines and be approved by Southern Health-Santé Sud's ICT Department.
- Malware Protection
  - Malware protection systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off, disable, or circumvent security and device protection. (e.g. anti-virus software, encryption etc.)
- Access Controls
  - Physical and electronic access to Confidential Information and computing resources is controlled. To ensure appropriate levels of access by a User, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by Manitoba eHealth. Mechanisms to control access to Confidential Information include (but are not limited to) the following methods:
    - Authorization: Access will be granted on a "need to know" basis and must be authorized by the User's Manager. The Application Owners reserve the right to approve/denial access based on specific criteria they lay out.
    - Identification/Authentication: Unique User identification (User ID) and authentication is required for all systems that maintain or access Confidential Information. Users will be held accountable for all actions performed on the system with their User ID. Southern Health-Santé Sud ICT Department is responsible for the establishment and maintenance of standards for Identification and Authentication.

- Data Integrity: Confidential Information within the Corporate Network will be protected from unauthorized modification, insertion, or deletion including during processing, transmission, and in storage.
- Transmission Security: Southern Health-Santé Sud ICT Department must ensure technical security mechanisms are in place to guard against unauthorized access to data that is transmitted over the Corporate Network.
- Remote Access: Access into the Corporate Network from outside will be granted using only Southern Health-Santé Sud ICT Department-approved devices and/or pathways on an individual User and application basis. All other network access options are strictly prohibited. Further, Confidential Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within Corporate Network.
- Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals. Southern Health-Santé Sud ICT Department will use security perimeters to protect areas that contain Data Centres supporting health applications. These secure areas will be protected by appropriate entry controls to ensure only authorized personnel are allowed access.
- Equipment and Media Controls: The disposal of information must ensure the continued protection of Confidential Information. The Southern Health-Santé Sud ICT Department disposal standards must be followed.
- External Media Controls: Confidential Information stored on external media (diskettes, cd-roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. The Southern Health-Santé Sud ICT Department must maintain and manage a standard for external Media which must be followed.
- Data Transfer/Printing/Electronic Mass Data Transfers: Downloading and uploading Confidential Information between systems must be strictly controlled. Requests for mass downloads for any purpose that include PHI must be approved through the Privacy Officer. For all other electronic data transfers and printing, Confidential Information must be stored in a manner inaccessible to unauthorized individuals. Confidential Information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PHI that is downloaded for educational purposes will be de-identified before use.

- Oral Communications on mobile devices: Southern Health-Santé Sud staff will be aware of their surroundings when discussing Confidential Information. This includes the use of cellular telephones in public areas. Southern Health-Santé Sud staff will not discuss Confidential Information in public areas if the information can be overheard. Caution will be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.
- Audit Controls: Southern Health-Santé Sud ICT Department will support an automated audit trail capability for logging noteworthy security related events, including logging of the individuals, processes, and/or components that were associated with the event, as well as the time the event occurred. Audit logs will be accessible to authorized personnel only. Audit logs will be protected from unauthorized access and modification and will be reviewed regularly. These reviews must be documented and maintained as per Southern Health-Santé Sud retention standards.
- Evaluation: The Southern Health-Santé Sud ICT Department will ensure that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection. (e.g. Vulnerability Scanning and Assessments)
- Contingency Plan: Southern Health-Santé Sud must ensure that it can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Confidential Information. This will include developing policies and procedures to address the following:
    - Data Backup Plan: data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information. Backup data must be stored in an off-site location and protected from physical damage. Backup data must be afforded the same level of protection as the original data
    - Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

- Emergency Mode Operation Plan: Each Business Owner must ensure that a plan is developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
- Testing and Revision Procedures: Procedures will be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.
- Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Information Security Incident Management

- Southern Health-Santé Sud will develop and maintain a detailed and up-to-date security incident response plan to identify and resolve information security incidents and minimize their business impact.
- Prevention - To reduce the likelihood of a compromise of Southern Health-Santé Sud ICT Assets, Southern Health-Santé Sud will implement baseline security controls and any additional controls identified through threat and risk assessments.
- Detection – Southern Health-Santé Sud will monitor the operations of its ICT Systems to detect anomalies in service delivery levels and security violations.
- Response - In the context of investigating ICT security incidents, Southern Health-Santé Sud will establish mechanisms to respond effectively to ICT security incidents and exchange incident-related information with designated agencies and facilities management in a timely fashion. Southern Health-Santé Sud will appoint a single point of contact for communications with respect to security incident response.
- Recovery - Southern Health-Santé Sud will develop procedures to resolve ICT security incidents and return compromised ICT System and their components back to normal mission status. Southern Health-Santé Sud is responsible for developing a business continuity plan, such that business can continue in the event that an ICT System is unavailable due to a security related incident.
- Investigation and Reporting - Southern Health-Santé Sud will investigate and report on IT security incidents and take corrective action to prevent future, similar incidents. The Southern Health-Santé Sud ISO, or designate, will report to the CIO and CEO, any security incident that, in their opinion, could have a serious impact on patient care, the security or integrity of the ICT Assets or on the business of the Southern Health-Santé Sud.

Compliance

- The Information Security Policy applies to all Users of Southern Health-Santé Sud information. Failure to comply with Information Security Policies and Standards may

result in disciplinary action up to and including dismissal in accordance with applicable Southern Health-Santé Sud procedures, or, in the case of outside affiliates, termination of the affiliation. Further, penalties associated with Provincial and Federal laws may apply.

DEFINITIONS:

Availability - Data or information is accessible and usable upon demand by an authorized user.

Business Owner - This role often corresponds with the management of an organizational unit responsible for the creation of a collection of information. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual (e.g. the primary user of that information).

Confidential Information – includes, but is not limited to: Personal health information as defined in the *Personal Health Information Act (PHIA)*; Personal information as defined in *The Freedom of Information and Protection of Privacy Act (FIPPA)*; Information contained in a clinical record as referenced in *The Mental Health Act (MHA);* and, Administrative records collected and created as part of the course of business of Southern Health-Santé Sud and relate to legal, financial and operational matters of a confidential nature.

Corporate Network - All computer equipment and network systems that are operated within the Southern Health-Santé Sud-managed environment. This includes all platforms (operating systems), all computer sizes (smartphones, tablets, desktops, servers, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

The Custodian - The Custodian of information is responsible for the processing and storage of the information. The Custodian is responsible for the security of controls as specified by the Information Security Officer and the Business Owner. Southern Health-Santé Sud ICT department and system administrators are the custodians of information.

Data Centre - Any facility used to house computer systems and associated components, such as telecommunications and storage systems. This includes data centres, wiring closets, telecomm rooms, and server rooms.

ICT Assets - Tangible or intangible assets relating to information technology including, but not limited to, all information (including Confidential information) in electronic form and the hardware, software or network components on which information is entered, processed, stored or transmitted.

ICT Security – Consists of the processes and mechanisms by which computer-based equipment/infrastructure, information and services are protected from unintended or unauthorized access, change, or destruction. It covers the CIA (Confidentiality, Integrity and Availability) of data through People, Process & Technology.

Personal Health Information (PHI) – recorded information about an identifiable individual that relates to: a) the individual's health, or health care history, including genetic information about the individual b) the provision of health care to the individual, or c) payment for health care provided to the individual; and includes: d) the Personal Health Identification Number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision or health care or payment for health care.

Risk - The probability of a loss of confidentiality, integrity, or availability of information resources.

User – Individuals who are authorized to access Southern Health-Santé Sud's ICT Systems

User Managers - Southern Health-Santé Sud management who supervise Users

REFERENCES:

The Personal Health Information Act, Government of Manitoba, In force December 11, 1997.
The Freedom of Information and Protection of Privacy Act, Government of Manitoba, In force May 4, 1998.
International Organization for Standardization (ISO)/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
ISO 27799:2008, Health Informatics – Security management in health using ISO/IEC 27002.