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.002 Program Area: Information and Communication Technology Policy Section: General
Issue Date: April 15 2019 Review Date: Revision Date:	Subject: Appropriate Use of Information and Communication Technology

POLICY SUBJECT:
Appropriate Use of Information and Communication Technology

PURPOSE:
To establish appropriate usage of Southern Health-Santé Sud Information and Communications Technology (ICT) systems.

BOARD POLICY REFERENCE:
Executive Limitation 1: Global Executive Restraint & Risk Management
Executive Limitation 7: Corporate Risk

POLICY:

- ICT resources are intended for business use only.
- Southern Health-Santé Sud reserves the right to monitor, review, access and/or block user activity without user notification.
- Users are responsible for all activity while logged in under their assigned network user ID and password.
- Any material created, stored, sent or received using ICT resources are considered the property of Southern Health-Santé Sud.
- All users have a legal and ethical duty to protect the confidentiality, integrity and availability of all electronic information.
- Access to information systems and data is restricted to authorized users and is limited to that which the user requires to do their job.
- Southern Health-Santé Sud will report and cooperate with law enforcement where activities or reports of activities are considered illegal.

- The ICT acceptable use policy extends to any on site or remote locations (e.g. working from home).

PROCEDURE:

- **Protecting ICT Resources**
  - Users apply appropriate precautions to prevent loss, damage, theft and/or unauthorized access to ICT resources.
  - Computer sessions are logged-off or locked when the user is away from the workstation, to prevent unauthorized access.
  - Individual passwords are never shared.
  - Only the user assigned user ID and password are used to access systems.
  - Compromised passwords are changed promptly and reported by phone to the eHealth service desk as a Critical Ticket.
  - Approval is obtained from ICT for use and/or installation of new software and hardware.
  - Suspicious files/programs or messages encountered while using ICT resources are reported to ICT.
  - Lost or stolen ICT resources are immediately reported to ICT.
  - ICT is contacted where ICT equipment is moved/relocated to another office/program/facility.
  - Intentional and/or malicious disruption to ICT services is prohibited.
- **Confidentiality**
  - Users are responsible for proper storage (e.g. secure network folder) and security of all confidential information.
  - Confidential information is not stored on a local computer (C:) drive or on any portable storage media unless it is encrypted and/or password protected. (Note: Information stored on a local computer (C:) drive or portable storage media is not protected by automatic back-up processes.).
  - Access to information stored in a network storage location is restricted to users who require the information to do their job.
- **Email**
  - Email is created and used in a professional manner.
    - Note: Email created in the course of carrying out Southern Health-Santé Sud duties are considered business records and access may be requested by any person under *The Freedom of Information and Protection of Privacy Act (FIPPA).*
  - Confidential information is not sent to an email address other than @southernhealth.ca unless it has been secured (e.g. Encrypted). If assistance is required contact ICT. Exceptions to this rule are:
    - Email is the <u>only</u> timely way to send information that is required urgently and informed consent has been documented and obtained from the appropriate individual.

        - The purpose is for scheduling appointments where the individual has requested or agreed to receive this information by email and has provided their email address
        - The organization receiving the email has an established secure connection with Southern Health-Santé Sud. ICT maintains and posts a current list of those organizations.
    - Users open only email and attachments from a trusted or verified source. Email attachments from unknown sources should be promptly deleted, unopened.
    - In the event of accidentally opening a suspicious attachment, report this by phone to the eHealth Service Desk as a Critical Ticket.
    - Confidential work related information is not forwarded to personal email addresses or any other non-work related accounts.
    - Email messages are not forged or altered to impersonate another individual or entity.
    - Email folders (e.g. Inbox, Sent) are managed by routinely deleting unnecessary items and/or the use of archive folders in accordance with ICT guidelines.
    - Email addresses and contact names are verified prior to sending/forwarding email messages.
    - Email that contains defamatory, offensive, racist or obscene remarks is prohibited and users, who receive an email of this nature, notify their supervisor/manager.
    - Email signatures must include a signature with the employee's name and position as well as the Southern Health-Santé Sud name and address. In addition, on any communications to non-Health Authority Computer Network, each email must include the Southern Health-Santé Sud-generated disclaimer. A more detailed description of Email signatures can be found in the Graphic Standards Manual – ORG.1110.PL.002.SD.01.
    - Use of spellchecker prior to sending email is strongly encouraged.
    - Sending/forwarding of chain letters, junk mail, mass personal mailings, alleged virus alerts or other SPAM is not permitted.
    - Forwarding jokes is discouraged.
- **Internet**
    - Confidential information is not transmitted over the Internet unless it has been secured (e.g. encrypted).
    - Accessing, viewing, downloading or distributing objectionable material is prohibited.
    - Unauthorized Internet use includes, but is not limited to:
        - audio and video streaming not required for work,
        - gaming,
        - peer to peer file sharing,
        - music downloading not required for work,
        - gambling

    - Due to the threat of malware, internet usage should be limited to known reputable sites or sites that are required as part of an employee's regular work.
    - Users will only connect to an identified wireless network where the source is known. For example, when in a hotel, use the hotels wireless connection provided to you. Do not connect to "unknown" or "suspicious" networks.
    - Social Media
        - Access to external social media sites may be blocked on the Southern Health-Santé Sud network. Users may be granted access to blocked sites for work-related business or for education purposes where authorized by their Manager\Director.
        - Users shall only access Social Media as outlined in the Social Media policy ORG.1510.PL.016.
- **Personal Use**
    - Personal use of ICT resources/services (e.g. email or Internet) is limited to break time and does not interfere with work.
    - Conducting or pursuing personal business interests or those of another organization while using ICT resources is prohibited.
    - Personal files stored on the network are routinely deleted.
- **Desktop and Portable Electronic Devices (PEDs)**
    - Screen savers are set to password protect the PED after a maximum of 20 minutes.
    - Users take steps to prevent unauthorized viewing of the computer screen/display.
    - PEDs are not left unattended unless physically secured.
    - A security cable is used for PEDs kept in unsupervised locations. Where a PED has no place to attach a cable, the device is placed in a secure storage location.
    - PEDs are stored in a secure location when taken home.
    - PEDs are not left in a vehicle.
    - When traveling by plane, taxi or train, verify that you have the PED and the case, including all contents, prior to exiting.
    - PEDs are kept in sight when going through airport security checkpoints.
    - Users only connect to an identified wireless network to which the source is known. For example, when in a hotel use the hotels wireless connection provided to you. Do not connect to "unknown" or "suspicious" networks.
    - PEDs are locked in the room safe, where provided by the hotel.
    - When photography, audio, or video recordings are required, if they contain personal or health information, they are to be managed on Southern Health-Santé Sud- owned PED's or other devices specifically designated for medical recordings, and treated as health or personal information in accordance with PHIA /FIPPA and applicable Southern Health-Santé Sud policies and procedures. Southern Health-Santé Sud representatives must not use a personal mobile device to record any photographs, audio, or videos for medical or other purposes. When required, these recordings must have prior written consent of all individuals being recorded.

  - Patients, clients and visitors using PED’s or other recording devices to take photographs, videos, or audio recordings in a Southern Health-Santé Sud facility are to be advised that they must respect the privacy of Southern Health-Santé Sud representatives and other patients and visitors who may not consent to being recorded, and must not collect health or personal information of other individuals in any recording.
  - Use of PED’s and two-way radios are permitted in non-restricted areas of Southern Health-Santé Sud facilities. PED’s that connect to a cellular network are to be turned off or set in “airplane mode” within one (1) meter of functioning medical devices in restricted areas. When two-way radios must be used, they must be at least three (3) meters away from functioning medical equipment when sending and transmitting in restricted areas. Restricted areas include, but are not limited to:
    - Critical/intensive care units;
    - Operating rooms;
    - Emergency departments;
    - Post anaesthetic recovery rooms;
    - Neonatal intensive care units;
    - Cardiac telemetry units; and
    - Other areas designated by the facility’s leadership.
  - Employees who suspect any medical equipment malfunction is being caused by electromagnetic interference are to ensure that the mobile device use is immediately turned off around the equipment and to report the incident. Equipment malfunctions related to electromagnetic interference may include, but are not limited to:
    - Apparent differences between a patient’s condition and the data provided by a medical device or monitor; and
    - Intermittent equipment malfunction or alarm signal during PED use.
  - Remote access to Southern Health-Santé Sud systems through Desktop Computers and PED’s must meet the standards established by Southern Health – Santé Sud ICT. Users must comply with the Remote Access to Corporate Network Policy -ORG.16110.PL.004.
- **Portable Storage Media**
  - Encrypted and/or password protected portable storage media are used for data transfer of confidential information.
  - Portable storage media is ordered through the ICT to ensure it meets ICT standards for secure devices.
  - Use of other types of personal portable storage media is discouraged and may be monitored and/or blocked.
  - Vendors and presenters using portable storage media are advised that the files on the device are subject to Southern Health-Santé Sud anti-virus scanning.
- **Privacy and Security Incidents**

- Immediate steps are taken to contain an incident by securing and/or recovering any compromised ICT resources.
- All incidents or potential compromise to the confidentiality, security, integrity or availability of ICT resources is immediately reported to the Regional Manager – ICT and/or Regional Manager – Privacy.
- Misuse of ICT resources/services by any user is reported to their immediate supervisor/manager.
- Users need to be aware that Southern Health-Santé Sud routinely monitors internet, email and file access. Management reserves the right to monitor and examine usage/content and/or block user activity without user notification in order to ensure compliance with this and other related policies.
- Users should be aware that electronic correspondence and messages (e.g. email, internet, social media, content in file storage, etc.) may be considered a record and therefore may be accessible to an applicant under the Personal Health Information Act (PHIA) and the Freedom of Information and Protection of Privacy Act (FIPPA); caution and discretion should be exercised by users.
- All Personal Health Information (PHI) whether managed in an electronic format, or hard copy transferred to an electronic format, will only be transmitted externally in accordance with the Privacy & Access - Security and Storage of Personal Health Information policy ORG.1411.PL.404. Consultation shall occur with the Regional Privacy and Access Officer, or designate, to determine the appropriate method of securing electronic files for transmission, as required.
- Electronic Personal information will only be transmitted externally in accordance with the Privacy of Personal Information under The Freedom of Information and Protection of Privacy Act (FIPPA) policy Org.1411.PL.007.

DEFINITIONS:

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*), and; Administrative records collected and created as part of the course of business of <Region/Organization> and relate to legal, financial and operational matters of a confidential nature.

Encryption: a method of converting data to a secure and unreadable format. Data can only be read by an individual who has the "key" to unscramble the code (e.g. a password).

ICT Resource Disruption: Disruptions include, but are not limited to:

- Propagation of computer viruses, worms, spyware, malware, Trojan horses, email bombs, etc.
- Disconnection of, or damage to equipment or services
- Disruption of network traffic causing loss of service, including excessive bandwidth or excessive use of computer resources
- Rogue modems and/or wireless access points
- Port scanning or security scanning

- Network monitoring that intercepts data not intended for the use outside normal job responsibilities
- Change to the system or data configuration that could affect system integrity

ICT: refers to the Information and Communications Technology department

Information and Communications Technology (ICT) Resources: all assets relating to information and communications technology including, but not limited to, all information in electronic form (e.g. personal health information) and the hardware, software or network components on which information is entered processed, stored or transmitted

Information and Communications Technology (ICT) Services: includes all Southern Health-Santé Sud internet, email, network and telecommunication services

Objectionable Material: includes but is not limited to:

- obscene or pornographic material
- hate propaganda or discriminatory material
- defamation and libel
- sexual harassment
- offending pictures and jokes
- messages where the meaning is likely to be highly offensive to the recipients of the message

Persons associated with Southern Health-Santé Sud: includes Southern Health-Santé Sud medical staff, contracted persons, volunteers, students, researchers, educators, and Board members.

Portable Electronic Devices (PEDs): include portable computers that may be referred to as a "laptop, "Notebook", "Netbook" or "Tablet"", Smart phones and other similar devices.

Portable Storage Media: hardware devices used to store information. This includes, but is not limited to USB storage devices (e.g. memory stick, flash drive), CD/DVD, etc.

Remote Location: a physical location outside your normal office or work location.

Security Incident: an action by an authorized or unauthorized user or an event that may negatively impact or cause interruption, unauthorized access, modification, destruction or denial of service

Privacy Incident: incidents where there the confidentiality, security, accuracy and/or integrity of confidential information has been compromised.

Social Media: Internet-based applications that allow the creation and exchange of user-generated content. This includes, but is not limited to websites such as Facebook, Twitter, YouTube, LinkedIn and MySpace.

Streaming: Connecting via the network to listen to radio stations or viewing videos or webcasts

Transitory/working emails/documents: Messages/documents of short-term use and significance that are not required as part of a required record maintenance system once read or superseded. (I.e. meeting requests, messages that are not required as evidence of the decision making process)

User: an employee, physician, contracted individual, student, volunteer, researchers, educator, or Board member who is authorized to use information communications technology resources.

User ID: a unique personal network/system identification (e.g. username).

Virus or Malware: any program designed to copy itself into other programs often resulting in the alteration/loss of data and/or the disabling of computers and networks

Electromagnetic Interference: An electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment.

REFERENCES:

Graphic Standards Manual – ORG.1110.PL.002.SD.01
Privacy of Personal Information under The Freedom of Information and Protection of Privacy Act (FIPPA) Policy - ORG.1411.PL.007
Security and Storage of Personal Health Information Policy - ORG.1411.PL.404
Social Media Policy - ORG.1510.PL.016
Information and Communication Technology Security, Policy - ORG.1610.PL.001
Remote Access to Corporate Network Policy - ORG.1610.PL.004
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.