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.004 Program Area: Information and Communication Technology Policy Section: General
Issue Date: April 15, 2019 Review Date: Revision Date:	Subject: Remote Access to Corporate Network

POLICY SUBJECT:
Remote Access to Corporate Network

PURPOSE:
To establish the appropriate and secure remote access to the Southern Health-Santé Sud computer network.

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

POLICY:

- Southern Health-Santé Sud utilizes secure remote access technology for authorized users to connect to the Southern Health-Santé Sud corporate network from a remote location.

- Southern Health-Santé Sud adopts the Manitoba eHealth Remote Access Security standard to safeguard all ICT Resources from potential exposure or damages as a result of unauthorized or inappropriate use of remote access. Damages include the loss or exposure of sensitive or confidential data, intellectual property, damage to public image, damage to critical Southern Health-Santé Sud internal systems, etc.

- Remote access software is approved and supplied by the Southern Health-Santé Sud ICT department to ensure security standards are met. The ICT department is responsible for installing software on Southern Health-Santé Sud devices and provide instructions for the installation of software on third party devices as needed.

- Use of remote access technology creates an extension of the Southern Health-Santé Sud network, and as such, users are subject to all the same rules, regulations and policies as

they relate to the protection of the confidentiality, integrity and availability of all electronic information and information systems. This includes but is not limited to statutory requirements under the *Personal Health Information Act (PHIA)*, the *Mental Health Act,* and the *Freedom of Information and Protection of Privacy Act (FIPPA).*

- Users must agree to the terms outlined in the Remote Access Service – Terms of Use Agreement ORG.1610.PL.002.SD.01.

- All access to the Southern Health-Santé Sud corporate network and systems is monitored and audited to ensure confidentiality and security policy compliance.

- The regional Privacy and Access Officer is consulted and determines if a privacy impact assessment or information manager/sharing agreement is required prior to the establishment of a remote access connection with a third party. Third party approval is contingent on the execution of appropriate information manager or sharing agreements, which outline the requirements for the protection of confidential information from such risks as unauthorized access, use, disclosure, destruction or alteration and the requirement to adhere to acceptable use practices and established standards.

- The ICT department coordinates regular review of remote access privileges to determine if:
    - Staff have been terminated or are no longer in a position that requires remote access.
    - User has not logged in for a period greater than [6 months].
    - Service or support contracts have ended.
    - A user is in violation of Southern Health-Santé Sud policy.

- **Approval Criteria**
    - Remote access from Southern Health-Santé Sud owned devices is role based and a request is completed using the Install, Add, Move and Changes (IMAC) using form IMAC (Install, Move, Add, Change) Form – ORG.1610.FORM.001 form. The following criteria is considered prior to approval being granted:
        - Staff:
            - Access to information systems is required for staff to work away the workplace.
            - Remote access is required to enable working after normal business hours.
        - Third Party:
            - Remote access is required to support authorized ICT Systems and appropriate Information Manager's/Sharing Agreement has been signed, as required.
            - Required access pursuant to an established information sharing arrangement with non-Southern Health-Santé Sud health care providers or health care organizations where an Information Sharing Agreement is in place.

DEFINITIONS:

Confidential Information: includes, but is not limited to, Personal Information as defined in *The Freedom of Information and Protection of Privacy Act (FIPPA*); Personal Health Information as defined in *The Personal Health Information Act (PHIA)*; 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.

Device: any computing device used to connect to the Southern Health-Santé Sud corporate network from a remote location using remote access technology. Devices may include, but are not limited to, computers, tablets, laptops or Smart phones. Southern Health-Santé Sud, staff or a third party may own these devices.

Information and Communications Technology (ICT) Resources: All ICT assets and ICT Systems 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.

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

ICT Systems: The information and communication technology hardware, software and network components that make up a computerized system.

Information Manager or Sharing Agreement: An agreement between Southern Health-Santé Sud and a third party for the protection of confidential information against such risks as unauthorized access, use, disclosure, destruction or alteration. These agreements are required where a third party may have access to confidential information as part of a contractual or business relationship with Southern Health-Santé Sud. This may include, but is not limited to other health care providers, a person or body that processes, stores or destroys personal/personal health information or who provides information management or information technology services.

Privacy Impact Assessment (PIA): a tool used to assess legislative compliance and risks to personal privacy associated with a program, initiative, system or project. Privacy impact assessments identify issues and risks associated with the collection, access, use, disclosure, retention, destruction and security of personal and personal health information.

Remote Access: use of the Internet to establish a connection to the Southern Health-Santé Sud corporate network from a remote location for the purpose of accessing Southern Health-Santé Sud information or information systems.

Remote Location: a location external to Southern Health-Santé Sud that does not have a direct connection to the Southern Health-Santé Sud corporate network.

Remote Access Technology: software, hardware, system configuration or other methods used for establishing a secure connection from a device in a remote location to the Southern Health-Santé Sud corporate network. This technology includes, but is not limited to:

Staff: all employees and persons associated with Southern Health-Santé Sud including: medical staff, students, educators, volunteers, researchers, contracted individuals, agency staff and board members.

Third Party: any person or group of persons affiliated with an organization that requires access to the Southern Health-Santé Sud Corporate Network to fulfill their job responsibilities pursuant to an information sharing or business agreement.

User: for the purpose of this policy includes staff and third parties (e.g. vendor) who has been approved and granted privileges to remotely access the Southern Health-Santé Sud corporate network as outlined within this policy.

SUPPORTING DOCUMENTS:
Remote Access Service – Terms of Use Agreement - ORG.1610.PL.002.SD.01
IMAC (Install, Move, Add, Change) Form