# Saskatchewan Cancer Agency

**DIVISION**: Corporate Services

**POLICY #: IMS - 0118**

**DEPARTMENT**: Information Management Services

**ISSUE DATE**: June 30, 2008

**CATEGORY**: Policy

**REVISED DATE:** April 3, 2018

**POLICY TITLE:** Remote Access Security Policy

---

**Policy Statement**

Permission may be granted to allow access to the Saskatchewan Cancer Agency's (SCA) applications and network data remotely from outside SCA's network using a remote access connection. SCA employees must use an SCA supplied computer for this purpose. External vendors and partners may use their own equipment provided it adheres to security standards as defined below in the procedure section. SCA reserves the right to revoke this privilege if the policies and procedures are not followed as outlined below. SCA employees, contractors, consultants, temporary and other workers at SCA must agree to the terms and conditions set forth in this policy in order to be able to utilize mobile devices to connect the SCA's systems.

**Purpose**

To ensure secure and trustworthy use of the SCA network when being accessed by remote users. Also policy is intended to protect the security and integrity of SCA's data and technology infrastructure. Failure to address remote access threats may result in loss of confidential information, sensitive information, PI, PHI and intellectual property, as well as damage to public image or SCA internal systems, etc.

**Application**

This policy and standards apply to all employees, contractors, consultants, volunteers, research staff, observers, students or temporary and other workers at SCA, including all personnel affiliated with third parties that utilize SCA owned devices that connect to SCA systems.

**Authority**

ELT

**Information**

Information Management Services
Human Resources – use off hours

| Approved By: _____ Signature | Date: May 29/18 |
|---|---|

**Definitions**

| | |
|---|---|
| Remote Access: | Any connection to SCA's network, remote access to clinical repositories (PIP, PACS, etc.) , where access privileges have been granted by and fall under the trusteeship of the SCA and/or other applications from off-site locations such as an employee's home, partner/vendor place of work, hotel room, airport, café, wireless device, etc. |
| Keylogger: | Malicious software that intercepts keystrokes. |
| Screen Scraper: | Malicious software that intercepts the information displayed on your screen |

**Procedure**

## 1. The use of Remote Access Security

**1.1.** Employment at the SCA does not automatically guarantee granting of remote access privileges. Remote access will be granted to users as deemed necessary on a discretionary basis, based on the minimum requirement for their functional user roles. SCA Reserves the right to remove remote access at any time.

- This policy supports and does not supersede the HR Confidentiality Agreement Policy or IMS-0002 Acceptable Use Policy. Vendors must agree to conform to Policy IMS-0109 External Service Provider Policy.

**1.2.** Any and all use of SCA data, network, applications and/or systems through a remote access connection (normally Citrix Access Gateway or, in special cases, a VPN) is covered by this policy. The following exceptions are not covered by this policy since there is no direct connection made to the internal SCA network.

- Blackberry email
- Outlook Web Access

## 2. Remote Access Requests

2.1. All request for remote access by SCA personnel is made via the Service Desk. The request should include a brief description of the business reason why this access is required. SCA reserves the right to restrict what systems or information are available via remote access.

- Requests for in-scope staff should indicate whether remote access is expected to be needed permanently or just for a period of time
- For non-managerial staff, the request must be approved by the requestor's manager and the CIO. Managers and Physicians may be granted access upon request.
- Managers wanting remote access for in-scope staff should be aware of relevant material in the collective Agreement regarding over time and HR-405 Home- Based Position Policy.
- Scenarios when in-scope staff may be considered for temporary access would include the following:
  - Staff on standby who do not need to be physically present to do their work.
  - Working from home during influenza pandemic.
  - Finishing specific projects on an overtime basis where on-site supervision is not required.

## 3. Security Requirements

3.1. The personnel may uses personal equipment for remote access, however IMS will not provide support for such equipment.

3.2. External vendors with support contracts and external health care partners (e.g. COPS Centers) may use their own computers, provided that they meet the following criteria:

- Must be kept up to date with security patches.
- Must have an anti-virus and ant-spyware program installed with up to date definitions.
- Must take every effort to ensure malicious Keylogger or Screen Scraper software is not installed on the computer. These types of programs transfer any information typed or viewed on the screen to third parties, usually with criminal intent (e.g. identity theft or financial fraud).

3.3. Remote users of SCA systems and data must take careful steps to obey Saskatchewan's privacy legislation such as *The Health Information Protection Act* and *The Local Authority Freedom of Information and Protection of Privacy Act*. Users must also conform to SCA's Information Privacy Policies, in particular IMS – 0101 Information Classification Policy. The following are of particular concern:

- All confidential information including personal or personal health information must never be printed outside the agency, including on home printers, or publicly accessible printers (e.g. printers in a public library or an internet café) as these devices have the capability of storing print jobs.
- Any information sent via email must comply with the Secure Electronic Confidential Transmission of Information Policy and applicable guidelines.
- Public cloud services (i.e. iCloud, Dropbox, etc.) have capabilities to store and retrieve files through third party storage facilities. Use of these public cloud services for storing confidential, personal or personal health information is prohibited.
- When viewing personal health information, users must take steps to ensure bystanders cannot view the computer screen or view the user's actions.

## 4. Right to Monitor User Activity

4.1. SCA reserves the right to monitor and audit user activity and data transmission that occurs during a remote access session. This includes user access to confidential information, sensitive information, patient information, or personal health information. Event logs record SCA user activities, exceptions, faults and information security events are kept and are subject to review.

**Related Policy**

IMS - 0001 Information Classification Policy

IMS - 0002 Acceptable Use Policy

IMS - 0109 External Service Provider Policy

HR – 405 Home – Based Position Policy

PRI – 0800 Protection of Personal/Health Information Policy

Supersedes or Replaces:

IMS – 001-18 Remote Access Security Policy

**References**

*The Health Information Protection Act*

*The Local Authority Freedom of Information and Protection of Privacy Act*