BC CANCER BREAST SCREENING
Provincial Health Services Authority

| | | | |
|---|---|---|---|
| **Policy Title:** | Computer and Laptop Use and Maintenance | | |
| **Section:** | Access to Information | **Reference No.** | SI 060 |
| **Effective:** | July 2011 | **Revision:** | February 2018 |

## 1. SCOPE

All Breast Screening Program Staff

## 2. POLICY

All staff must ensure at all times the safeguard of PCs, laptops, and networks (e.g. Citrix) especially those that contain any sensitive and confidential information and data. All Breast Screening program staff that have access to PHSA/Screening Program PCs, laptops and networks is to abide by all PHSA policies regarding computer use, handling and maintenance, etc. The PHSA policies and procedures can be accessed through the POD (PHSA on Demand) website (copies attached).

## 3. PROCEDURE

When work areas are to be left unattended, sensitive or confidential materials must be cleared from view and unauthorized access. The following must be followed in order to ensure that PCs, laptops, and confidential or sensitive PHSA information is not left vulnerable to unauthorized use and disclosure:

1. Before leaving a work area:

   a) Tidy up the work area so client information or confidential materials are not vulnerable to unauthorized viewing.

   b) PCs and laptops must be locked or completely shut down when not in use.

   c) Client information and confidential documents and computer media must be stored in secure locations. This includes but is not limited to:
      - User IDs and password information
      - Centre day sheets
      - Client files (MA reports, client surveys, etc.)
      - Account numbers

2. Laptops must be kept with the user or in a secured area or container when not in use.

3. Any emails and/or files containing client / confidential information must not be saved on the PC or laptop’s hard drive.

4. Users must never store any confidential or client information on the hard drive of their home computer or other personal computing device.

5. Users must not share a PC or laptop used for working with PHSA sensitive and/or share confidential information with other individuals, including family members and friends.

6. Users must avoid viewing personal or confidential information in public, including while traveling on airplanes, trains, buses and public transit.

7. All users must change their password regularly to ensure security.

8. Using external email sources such as Hotmail, Yahoo or other non-PHSA / BC Cancer email accounts to access or transmit PHSA / BC Cancer / Breast Screening program data, records or information is prohibited.

## 4. RELATED POLICIES

SI 050 – Access to Breast Screening Application

PHSA policies:

- IMIT Securing PHSA Electronic Data
- IMIT 110 - Network Acceptable Use
- IMIT 140 - Internet and Electronic Mail Messaging
- IMIT 170 - Computer Equipment, Electronic Data Loss, Damage or Theft
- PHSA Remote Access
- PHSA Information Security
- PHSA Mobile Computing and Portable Storage Device Security
- IMIT 210 - Clear Desk and Screen

## 5. RESPONSIBLE PARTY

Screening Operations Director