Mobile Computing & Portable Storage Device Security

“Organization”, as referenced below, is defined as the Provincial Health Services Authority (PHSA) and / or Vancouver Coastal Health (VCH) and / or Providence Health Care (PHC).

1. Policy Purpose

Mobile Computing and personal storage devices are important tools for improving or enhancing performance of professional duties at work onsite, offsite, or at home. These devices require additional security awareness and measures in order to protect Confidential or Personal Information and information resources.

Staff may work in uncontrolled locations such as hotels, airports and other public spaces. Usage of mobile computing or portable storage devices in uncontrolled areas increases information security risks, with regards to wireless networking, access control, and malicious code prevention.

The Mobile Computing & Portable Storage Device Security Policy (the “Policy”) is to ensure that:

- Confidential or Personal Information, is protected while mobile computing and using of portable storage devices.
- Information on portable storage devices is protected to the level indicated by the sensitivity of the information stored on the device.

2. Policy Statement

2.1. Use of Mobile Computing and Portable Storage Devices

a. Confidential or Personal Information must be kept under staff control at all times; if this is not possible, the information must be stored securely to prevent theft, loss, damage or disclosure.

b. If there is a legitimate business need to store Personal Information on mobile computing or portable storage device the information must be stored for the absolute minimum time required, and deleted after usage.

c. Personal Information must be maintained and protected in accordance to the Mobile Computing & Portable Storage Devices Security Standard.
d. If Confidential or Personal Information is stolen, damaged or lost, staff must immediately notify the Help Desk and their direct Manager, Supervisor and/or Delegate. The Help Desk informs the Information Privacy Office.

2.2. Device Requirements

a. Whenever possible, staff should only use corporate managed mobile and portable storage devices.

b. Staff may use personal computers, mobile computing devices and/or portable storage devices in the workplace only if authorized by the organization (approval from an authorized personnel and/or Delegate).

c. Upon approval by a Manager, Supervisor and/or Delegate, personal devices must be registered with HSSBC.

d. Confidential or Personal Information must be encrypted on all mobile and portable storage devices.

2.3. Responsibilities

Staff are responsible for:

a. Protecting mobile computing devices against unauthorized access by using controls such as passwords, encryption and multi-factor authentication technology.

b. Allowing configurations and applications to be applied to personal devices for the purposes of meeting security and privacy obligations.

c. Protecting mobile devices and portable storage devices from loss, theft and unauthorized access by keeping devices locked in secure environments when not in use.

d. Reporting any loss or theft of a mobile device to the Organization.

e. Ensuring that personal mobile computing devices connected to the organizations’ networks meets the standards defined by the Remote Access Security Standard.

f. Disconnecting remote access sessions when not in use.
g. Not sharing their remote access mechanisms, credentials, or login information.

h. Ensuring that only secure and appropriate electronic sharing features are enabled to avoid unintentional disclosure as guided by the Mobile Computing & Portable Storage Devices Security Standard.

i. Avoiding verbal, visual or any other means of disclosure of Confidential or Personal Information in public, including but not limited to such public settings as buses, commuter trains, subways, airplanes, restaurants or street.

j. Creating an inventory of all Confidential or Personal Information stored on mobile computing devices and portable storage devices. This list should NOT be kept on the device itself.

k. Ensuring that all mobile computing and portable storage devices are registered or “known” prior to connection on either local (LAN), or wireless (WLAN) corporate networks.

The Organization is responsible for:

a. Ensuring that controls are defined for monitoring and auditing mobile computing and portable storage device usage

b. Defining, approving, and updating mobile computing and portable storage device security controls and appropriate use policies

c. Ensuring that appropriate staff education, and communication processes are in place for distribution of service changes and outage dates.

HSSBC is responsible for:


d. Implementing controls to monitor and audit mobile computing and portable storage device use

e. Supporting the organization with development and review of policies and standards

f. Managing and maintaining corporate mobile computing and portable storage devices

g. Reporting issues regarding mobile computing, portable storage devices and services to the organization

This material has been prepared solely for use within the Organization (Provincial Health Services Authority and/or Vancouver Coastal Health Authority and/or Providence Health Care). The Organization accepts no responsibility for use of this material by any person or business not associated with the Organization. A printed copy of this document may not reflect the current, electronic version on the Organization’s Intranet.
3. **Policy Scope**

This policy applies to:

- All Staff who use mobile computing and portable storage devices that access Confidential and Personal Information;
- All mobile computing and portable storage devices connecting to corporate information resources containing personal, confidential or sensitive information;
- All Staff involved in approving and administering mobile devices.

4. **Policy Principles**

4.1. Management of Confidential or Personal Information must be done in a manner that does not compromise the security and integrity of Systems, staff, patients, or families, in accordance with the law.

4.2. Mobile devices are only provided to staff with a legitimate business need to work outside the organization’s network.

4.3. Staff are accountable to minimize the security risks associated with their usage of mobile computing and portable storage devices.

4.4. The organization’s mobile computing and portable storage devices conform to industry and commonly accepted standards and best practices.

5. **Procedures**

Staff should follow the process as defined by the Organization, for additional information see the **Mobile Computing & Portable Storage Devices Security Standard**, **Remote Access Security Standard** and Guidelines for Registering Personal Devices.

6. **Exceptions**

Exceptions to this Policy are only permitted in extraordinary circumstances for approved business or clinical purposes and when the exception is supported by a security risk assessment.

Exceptions to the “Mobile Computing & Portable Storage Device Security” policy must be approved by the Chief Information Officer, IMITS. Approval is contingent upon a
formal request and a security threat and risk assessment. Any approved exceptions must be re-evaluated regularly, or whenever a material change to the control environment occurs. The business sponsor is responsible for notifying HSSBC of any changes to the control or operating environment described in an approved exception.

Exceptions to the “Mobile Computing & Portable Storage Devices” policy for certain parameters may not be possible for all Staff or Systems.

7. **Internal Tools, Forms and References**

8. **Related Policies**
   - Acceptable use of Technology Policy
   - Access Management Policy
   - Controls for Malicious Code Policy
   - Information Security Classification Policy
   - IT Security Policy
   - Network Security Policy
   - Management of Standard Software Patches Policy
   - Monitoring & Logging Policy
   - Remote Access Policy
   - Wireless (WiFi) Network Policy

9. **Definitions**
   
   “**Confidential Information**” means information and data, in any form or medium, relating to the Organization, its business, operations, activities, planning, personnel, labour relations, suppliers and finances that is not generally available to the public, including Personal Information and information that is identified as Confidential Information in accordance with the Organization’s policies.

   “**Devices**” means an asset that remotely connects to and access corporate information and resources include, but are not limited to, smartphones (ie. BlackBerrys, android devices, iPhones), tablets, laptops, computers, or PDA’s.
“FIPPA” means the British Columbia *Freedom of Information and Protection of Privacy Act* as amended from time to time (see reference).

“HSSBC” means the Organization “Health Shared Services BC”. This is a division of the Provincial Health Services Authority, and it supports integrative and efficient, non-clinical services for all six health authorities in BC.

“Information resources” means information and technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated IT assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants).

“IMITS” means the Organization’s Information Management/Information Technology Services department.

“Least Privilege” means the security principle that ensures that a Staff should have only those privileges required for the task at hand and no more.

“Mobile Computing” means using a portable device with a wireless connection, in an area that is not-predefined onsite in the organization, including offsite locations. mobile computing devices include, but are not limited to, smartphones (ie. BlackBerrys, android devices, iPhones), tablets, laptops, computers, or PDAs. Often times these devices will be able to remotely connect to and access corporate information and resources.

“Multi-factor Authentication” means a system wherein more than one factor is used in conjunction to authenticate. Common factors of authentication include: something a user knows (i.e. a password), something a user has (i.e. a token), and something a user is (i.e. a fingerprint or retina pattern). Using multiple factors as opposed to one factor generally delivers a higher level of authentication assurance.

“Personal Information” means any recorded information about an identifiable individual (including, but not limited to patients, clients, residents, volunteers, students, staff, physicians or members of the public), but it does not include business contact information (business contact information is information such as a person’s title, business telephone number, business address, email or facsimile number).

“Portable storage devices” means compact devices that have the ability to store data and can be transported easily with the user. They include, but are not limited to, hard drives, flash drives (i.e. USB drives), SIM cards, memory cards (ie. SD card, SDHC, micro-SD compact flash), floppy disks, dvds, cds, or any type of storage media.
“Remote access mechanism” means a software, hardware, system configuration or other methods used to enable remote access including hardware tokens, digital certificates, and VPN configurations.

“Security Threat and Risk Assessment” means a component of a risk analysis specifically aimed at identifying security exposures.

“Staff” means all officers, directors, employees, contractors, physicians, health care professionals, students, volunteers and other service providers engaged by the Organization or organizations with which the Organization has concluded a network services agreement or any other authorized User.

“Standards” means a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition.

“Systems” means any of the Organization’s respective or shared electronic information system.

10. **External References**

- **BC Freedom of Information and Protection of Privacy Act**

- **BC E-Health (Personal Health Information Access and Protection of Privacy) Act**

- **Information Security Branch, Office of the Chief Information Officer, Ministry of Citizens’ Services, Province of British Columbia**

- **ISO 27002 Standards: Code of Practice for Information Security Management**
  - [http://www.27000.org/iso-27002.htm](http://www.27000.org/iso-27002.htm)