16.0 Information Management

16.4 Organization and Security

16.4.2 Protection

16.4.2.4 Remote Access

1.0 Purpose

The Vancouver Island Health Authority (VIHA) is committed to providing timely access to information key to the delivery of healthcare on Vancouver Island. The ability to provide remote access to VIHA information systems is paramount to ensuring healthcare data is available where and when it is needed to inform clinical decisions. The purpose of this policy is to define the requirements and standards for remote access to VIHA information systems.

2.0 Scope

This policy applies equally to all individuals associated with the VIHA (collectively defined as "Individuals") including:

- Employees of the VIHA, and those involved with its affiliated programs and agencies, including students;
- CEO, executives, management, and supervisory employees;
- Members of the VIHA Board of Directors;
- Volunteers of the VIHA;
- Staff on contract;
- Physicians with privileges at any VIHA site;
- Medical staff including physicians on contract, residents, and clinical trainees;

- University faculty and support staff who work at VIHA facilities; and
- Any authorized user of VIHA information systems or information in the custody and control of VIHA.

3.0 Policy

Individuals remotely accessing VIHA information systems must:

- Actively protect VIHA information and information technology assets;
- Comply with all applicable policies, procedure and laws;
- Protect information from inadvertent or deliberate disclosure to unauthorized individuals at the remote location;
- If wireless networking will be used at the remote location, ensure that it meets or exceeds current industry encryption and security standards;
- Immediately report security events or unusual activity;
- Permit VIHA to monitor and investigate security events at the remote location, including access to equipment used for remote access;
- Permit VIHA to audit compliance with this policy
- Maintain physical security of the device while remotely connected to VIHA information systems;
- Ensure that devices are not left unlocked and unattended while remotely connected to VIHA Information Systems;
- Logoff promptly upon completion of a remote access session;
- Ensure sensitive information is encrypted when transmitted over public networks;
- Ensure sensitive information in VIHA's custody and control is stored within VIHA information systems and not on a personal device;

All individuals have a responsibility to report violations of this policy without fear of reprisal. Individuals deemed responsible for violations of this policy may be subject to penalty or sanction up to and including termination of employment, cancellation of contract or services, termination of the relationship with VIHA, withdrawal of privileges and/or legal action.

4.0 Standards

The following risks inherent to remote access must be assessed prior to granting such access:

- The sensitivity and classification of information that may be accessed or stored at the remote location;
- The physical security of information, information technology assets and the remote
- location;
- Unauthorized information access by people at the remote location, either inadvertent or deliberate.

The following protection technologies and controls must be implemented on devices used to remotely access VIHA information systems:

- Unauthorized network access to the devices must be prevented through implementation of a firewall or filtering technology to protect against attack (e.g., to prevent network attacks against the device).
- Devices must be protected against *mobile* and *malicious code* using antivirus software enabled in real-time protection mode and updated daily.
- Devices must utilize a current, supported operating system with security patch levels not more than one month out of date;
- Transmission or storage of sensitive information must utilize an industry standard encryption algorithm (SSL, AES, 3DES etc) with a minimum key length of 128 bits.
- Access control permissions must be applied to prevent unauthorised access to information by system users;
- Sensitive information in VIHA's custody and control must not be stored on a personal device; and
- Physical security of the device must be maintained while remotely connected to VIHA information systems.

5.0 Definitions

Information: Any operational data or information gathered, processed transmitted or presented using a computer is defined as Information. This includes confidential personal health information and business related information.

Information Systems: Any electronic device or equipment used to support the electronic storage, transfer, or access of information.

6.0 Additional References:

1. VIHA Policy 16.4.2.1. Security of Electronic Information
2. VIHA Policy 16.4.2.2. Security of Health Records
3. VIHA Policy 16.4.2.3. Acceptable Use
4. VIHA Policy 16.4.2.5 Mobile Computing
5. VIHA Policy 1.5.1. Confidential Information – Privacy Rights of Personal Information
6. Freedom of Information & Protection of Privacy Act. R.S.B.C. 1996, c. 165