



16.0 Information Management

16.4 Organization and Security

16.4.2 Protection

16.4.2.3 Acceptable Use of Assets and Resources

1.0 Purpose

The Vancouver Island Health Authority (VIHA) delivers many information systems and services providing timely access to information key to the delivery of healthcare on Vancouver Island.

The purpose of this policy is to:

- Communicate expectations for the acceptable use of VIHA information systems.
- Prevent risks to network security and performance.
- Protect the privacy, confidentiality and security of VIHA's information.
- Increase adherence to VIHA information and technology-related legislation, policies and standards.
- Promote public trust in VIHA's use of information and technology assets.

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

All users of VIHA's information and technology resources must take responsibility for, and accept the duty to, actively protect information and technology assets. This includes taking responsibility to be aware of, and adhere to, all relevant legislation, policies and standards. VIHA uses information technologies to support employees and other authorized users to work efficiently in delivering healthcare services. Proper use of these technologies assists in the daily management of information, saves time and money, reduces administrative overhead and improves service delivery. The technologies include, but are not limited to, information systems, services (e.g., web services; messaging services); computers (e.g., hardware, software); and telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants). Improper use may jeopardize the confidentiality, integrity and availability of VIHA's information and technology assets, and may put personal information protection, security or service levels at risk.

Appropriate Use of Information Technology:

1. Individuals must use VIHA-provided or authorized information technology resources as the business tools required to do their work and provide efficient service delivery.
2. Users must use information and technology resources in accordance with published service level agreements and applicable terms and conditions. The following conditions, and others that may be established by VIHA from time to time, apply to all individuals:

Individuals must not:

- Attempt to circumvent or subvert system or network security measures;
- Propagate viruses knowingly or maliciously;
- Detrimentially affect the productivity, integrity or security of VIHA systems;

- Access a personal external email account (e.g., Hotmail) from a VIHA workstation for reasons unrelated to VIHA business;
- Access social networking websites (e.g. Facebook, MySpace) for reasons unrelated to VIHA business;
- Obtain or distribute files from unauthorized or questionable sources (e.g., racist material, pornography, file swapping sites);
- Access Internet sites that might bring the public service into disrepute or harm VIHA's reputation, such as those that carry offensive material;
- Access radio stations or video clips (typically referred to as "streaming" audio or video) over the Internet, unless the access is work-related and approved by a VIHA manager;
- Download non-work related files, such as Freeware, Shareware, movie or music files;
- Divulge, share or compromise their own or another's VIHA authentication credentials;
- Transmit or otherwise expose sensitive or personal information to the internet;
- Use information and technology resources for commercial solicitation or for conducting or pursuing business interests unrelated to the delivery of healthcare;
- Distribute hoaxes, chain letters, or advertisements;
- Send rude, obscene or harassing messages;
- Send, forward and/or reply to large distribution lists concerning non-VIHA business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists; and
- Attempt to obscure the origin of any message or download material under an assumed internet address;
- Knowingly enable inappropriate levels of information access by others; and
- Disclose any information you do not have a right to disclose.

Individuals must:

- Comply with all applicable legislation, regulations, policies and standards;
 - Use all appropriate anti-virus precautions when accessing non-VIHA data and systems from the VIHA network;
 - Adhere to licensing agreements for all software used;
 - Respect copyright and other intellectual property rights in relation to both programs and data;
 - Only use the email account provided by VIHA when conducting VIHA business over email;
 - Use approved security measures when accessing the VIHA network from home or a non-VIHA computer;
 - Only use messaging forums (e.g., Internet Relay Chat, internet newsgroups, social networking sites) when conducting work-related business or exchanging technical or analytical information; and
 - Use the rules for complex passwords to create password.
3. Any content created or transmitted using VIHA equipment or retained within the VIHA network may be monitored, captured and/or be subject to FOI requests.

4. All individuals have a responsibility to report violations of this policy without fear of reprisal. Inappropriate use of VIHA information technology resources will be investigated on a case-by-case basis. 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 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.

5.0 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 1.5.1. Confidential Information – Privacy Rights of Personal Information
4. Freedom of Information & Protection of Privacy Act. R.S.B.C. 1996, c. 165