Acceptable Use of Information Technology

1. Introduction

Description

Information Technology enables VCH to deliver health care services efficiently and effectively and to provide corporate support services. If used inappropriately, the same technology and resources may pose significant risks to VCH, its Staff, patients and clients and to the security of the Information Technology.

The purpose of this Acceptable Use of Information Technology Policy (the "Policy") is to define acceptable conduct and practices for all Users of Information Technology in order to:

- Ensure that the use of Information Technology is consistent with the VCH mission and values.
- Ensure that the use of Information Technology complies with professional and ethical obligations and provincial and federal laws.
- Protect VCH, its Staff, patients and clients from illegal, damaging or otherwise unacceptable activities (such as intimidation or harassment).
- Respect individual privacy rights.
- Safeguard VCH Information Technology assets.

Scope

This policy applies to all Users and all Information Technology.

Exceptions

Exceptions to this Policy may be made in extraordinary circumstances for approved business or clinical purposes, subject to approval of the Chief Financial Officer. Where there is significant risk to VCH, exceptions must be approved the Senior Executive Team. Any exceptions must comply with applicable law.

2. Policy

2.1. Responsibilities and Accountabilities

2.1.1. Information Management Information Technology Systems (IMITS)

IMITS including IMITS Security Services is responsible for:

(a) maintaining and administering this Policy;

(b) implementing safeguards to protect Information Technology from accidental or intentional misuse;

(c) providing cost-effective monitoring and compliance mechanisms in support of this Policy;

(d) developing additional guidelines for permitted and prohibited practices under this Policy;

(e) auditing and monitoring use of Information Technology.

2.1.2. Management

Management is responsible for:

(a) Ensuring that access to Information Technology is provided to Users only as required for job responsibilities;

(b) Ensuring that use of Information Technology complies with this Policy.

2.1.3. Staff

Staff is responsible for ensuring that their use of Information Technology complies with this Policy.

2.1.4. Information Privacy Office

Information Privacy Office is responsible for providing guidance on privacy requirements for system access and privacy compliance.

2.2. Ownership of Technology and Records

Information Technology and records generated, handled and stored by Information Technology (including duplicate or back-up copies) are the property of VCH or VCH/PHC in respect of shared systems, except as specifically agreed upon in writing with Staff, or as set out in approved VCH intellectual property policies or third party agreements. In particular, VCH may have agreements with other organizations, such as the University of British Columbia (UBC), which provide that the intellectual property policies of that organization will apply to certain Staff unless there is agreement to the contrary. All messages (including e-mail) generated on or handled by Information Technology are the property of VCH.

2.3. User Authorization

Before using any Information Technology, Users must obtain authorization from the appropriate VCH staff or representative for the Information Technology required. Users may not access or use Information Technology unless explicitly authorized by VCH.

2.4. Authorized Purpose

Users may only use Information Technology for authorized purposes in accordance with sections 2.5 and 2.6 of this Policy.

2.5. Business/Work Related Purposes

Information Technology may only be used for:

(a) the performance of job duties and legitimate VCH or VCH/PHC business purposes; and

(b) incidental personal use, provided it does not violate the employment obligations of the member of Staff and complies with section 2.6 "Personal Purposes".

2.6. Personal Purposes

Information Technology may be used for limited, incidental personal purposes provided the following conditions are met:

(a) use must be infrequent and of short duration, be reasonable and conform to commonly accepted standards of workplace, professional and ethical behavior;

(b) use is permitted by the individual's manager or supervisor and does not detract from the User's performance of his or her job duties;

(c) use does not compromise the performance of Information Technology or related services;

(d) use does not impede or adversely affect VCH or VCH/PHC administrative and business processes;

(e) use does not compromise the integrity or security of Information Technology;

(f) use does not expose VCH to costs or risk;

(g) use is not part of an activity which the User does for personal profit;

(h) User complies with any specific prohibitions of use of Information Technology established by VCH policies; and

(i) use otherwise complies with the rest of this Policy and related policies and guidelines, including the Internet Access Policy.

2.7. Terms of Use and System User Guides

Users must comply with any Terms of Use or User Agreements applicable to Information Technology that they have been authorized to use. Users should also comply with any user guides, manuals, instructions or training materials that provide guidance on the proper usage of Information Technology.

2.8. Representation of VCH

All external representations made on behalf of VCH or public disclosure of information concerning VCH via the Internet must be approved by VCH Communications and Public Affairs and as necessary General Legal Counsel. This includes, but is not limited to, information such as financial performance, information relating to staff or medical staff, facilities and others. Making fraudulent offers of services, products, items, Information Technology or other VCH or VCH/PHC assets is prohibited.

2.9. Copyright and Other Intellectual Property Rights

Users of Information Technology must respect and comply with all copyright, patent, trade-mark and any other intellectual property restrictions and conditions contained in applicable product purchase, service or licensing agreements.

2.10. Information Privacy

Staff shall ensure that they protect Personal Information when using Information Technology in compliance with the VCH Information Privacy and Confidentiality Policy and related privacy policies.

2.11. Security

Security is the responsibility of every User. The security of Information Technology depends on the appropriate use of these resources.

Users must:

(a) take all reasonable steps to ensure that VCH and VCH/PHC Confidential Information and Personal Information is protected from unauthorized use or disclosure. Users are expected to read and understand the User Security Guidelines;

(b) use security controls appropriately, including User ID's and passwords, cable locks, anti-virus software and following security policies; and

(c) take all reasonable steps to ensure that any VCH or VCH/PHC Information Technology device assigned to them such as a computer, laptop or BlackBerry, is protected from potential theft or loss at all times.

2.12. Prohibited Activities

Users may not use Information Technology or information in a manner that violates VCH policies, ethical obligations or the law. Prohibited activities are set out in the List of Prohibited Activities. Users are expected to read and understand the Prohibited Activities List.

2.13. Compliance and Monitoring

Users should not expect privacy when using Information Technology, which may be monitored by VCH in accordance with this Policy. However, VCH recognizes that its right to monitor Information Technology is not absolute. VCH monitors activities appropriate to risks and conducts monitoring in a reasonable manner.

VCH may employ various technologies to enable monitoring of activities. BC Clinical and Support Services (BCCSS) Security Services shall consult with the Information Privacy Office with respect to the nature of the technologies and proposed use to ensure compliance with applicable privacy laws and standards. VCH shall implement policies, guidelines and procedures with respect to monitoring, related data storage and retention.

2.14. Purposes of Monitoring

Subject to section 2.13, VCH may, with or without prior notice to Users, examine and filter hard drives, electronic mail messages, web browser cache files, web browser bookmarks, network transmissions, and other information stored on or transmitted through Information Technology for the purposes of:

(a) investigation of an actual or suspected breach of VCH policies;

(b) monitoring compliance with this Policy and related policies; or

(c) monitoring use and performance of Information Technology.

Designated Staff from IMITS or BCCSS Security Services, Legal Services and Employee Engagement may review audit logs and other records on Information Technology systems on a need to know basis for these purposes.

2.15. Reporting Violations and Discipline

Users are required to report any observed or suspected inappropriate use of Information Technology or information to the BCCSS Service Desk. Where possible, VCH will keep the identity of the individual reporting and the report strictly confidential. See section 2.16.1 "Reporting Violation Procedure".

If reporting to the Service Desk is not appropriate, Users may call the Whistleblower hotline to report observed or suspected inappropriate use of Information Technology or information. (see Whistleblower policy)

Any User found violating this Policy is subject to discipline including, but not limited to, loss of computing privileges, prosecution, dismissal for cause or termination and may be held liable for costs or damages incurred by VCH.

2.16. Procedures

2.16.1. Reporting Violation Procedure

Any User who believes that there has been a violation of this Acceptable Use of Technology Policy must contact Service Desk to report the incident. Unless there is immediate risk to VCH, its Staff, patients or clients, the User's manager or supervisor must authorize the investigation into an actual or suspected misuse of Information Technology before it proceeds.

If reporting to the Service Desk is not appropriate, Users may call the Whistleblower hotline to report observed or suspected inappropriate use of Information Technology or information. (see Whistleblower policy)

If available, the User or manager/supervisor shall provide the following information:

- The User's name or user-ID associated with the alleged violation
- The VTAG number associated with the alleged violation

- The date and time of the alleged violation
- Any evidence of the alleged violation

2.16.2. Reporting an Information Privacy Violation

Any actual or suspected violations of information privacy must be reported to the Information Privacy Office. Users must follow procedures outlined in Management of Information Privacy Incidents Policy.

2.17. Principles of Acceptable Use

(a) Information Technology must be used to support duties of employment or engagement. VCH requires that all Users of Information Technology do so in a legal, ethical and responsible manner.

(b) Access to Information Technology is made available to Users provided they comply with VCH policies, professional ethical obligations and applicable laws.

(c) Records stored on Information Technology are the property of VCH and/or PHC.

(d) Inappropriate use of Information Technology negatively impacts the ability of VCH to achieve its objectives and may create risk to VCH, its Staff and patients or clients.

(e) Monitoring of activities using Information Technology may be necessary to address risks, but must be reasonable both in respect of the nature of the monitoring and the manner in which it is carried out.

(f) Maintaining effective Information Technology security is the responsibility of all Users who have access to Information Technology.

3. References

Tools, Forms and Guidelines

- List of Prohibited Activities
- User Security Guidelines

Related Policies

- Corporate Identity and Branding
- Emailing
- Respectful Workplace and Human Rights
- Information Privacy and Confidentiality
- Information Privacy Breaches, Reporting and Management of

- Internet Access
- Media Policy and Procedures
- Standards of Conduct, Conflict of Interest and Whistleblowing Protection
- Telecommunication Services and Devices, Use of

Keywords

Acceptable use, information technology, confidential information, personal information, terms of use, user agreement, IMITS, BCCSS

Definitions

"**Confidential Information**" includes information and data, in any form or medium, relating to VCH, its business, operations, activities, planning, personnel, labour relations, suppliers and finances that is not generally available to the public and information that is identified as Confidential Information in accordance with VCH policies.

"**Information Technology**" means computer hardware and software and other technology used in the storage, processing, management and communication of information including, but not limited to, desktop and laptop computers, servers, the VCH/PHC network, clinical information systems, electronic mail and messaging, the Internet, the Intranet, voice mail, printers, facsimiles (fax), photocopiers, scanners, telephones, cellular phones, Blackberrys, video conferencing equipment, video cameras, digital cameras, hard drives, USB flash memory sticks and other portable storage devices owned, leased, licensed or controlled by VCH or VCH/PHC.

"**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).

"**Staff**" means all officers, directors, employees, contractors, physicians, service providers, health care professionals, students and volunteers engaged by VCH.

"**Terms of Use**" (otherwise referred to as "User Agreements") means the terms of use applicable to use of Information Technology systems, which may be in online or paper format.

"**User**" means any Staff or individual who has been authorized to access and use VCH or PHC Information Technology.

"**VCH**" means Vancouver Coastal Health Authority and in respect of shared Information Technology, "VCH/PHC" means VCH and Providence Health Care Society

Questions

Contact: BCCSS Service Desk or IMITS

Issued by:

Name: **Duncan Campbell** Title: CFO and VP, Systems Development and Performance Date: June 5, 2009

Signature of issuing official

Appendix 1: IMITS List of Prohibited Activities

Prohibited activities using Information Technology include, but are not limited to, the following activities:

1. *Illegal Use*

   Using Information Technology to create or transmit any material (by email, uploading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable local, provincial, national or international law is prohibited.

2. *Threats*

   Using Information Technology or assets to create or transmit any material (by email, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property is prohibited.

3. *Misrepresentation of VCH/PHC*

   Using Information Technology in a manner that misrepresents or may misrepresent the views, services or policies of VCH or PHC is prohibited. All communications purporting to represent the views or policies of VCH or PHC to the public must be pre-approved by VCH Communications and Public Affairs. Unless it is a part of normal job duties, making statements or representations, express or implied, about VCH or VCH/PHC services is prohibited unless authorized by VCH.

4. *Unauthorized Disclosure*

   Using Information Technology in a manner that results in or is likely to result in the unauthorized disclosure of Confidential Information is prohibited.

5. *Cause Harm*

   Users must not use Information Technology in a reckless or other manner that is intended or is likely to cause harm to Staff, patients, clients or others or to VCH or PHC property.

6. *Offensive Material*

   Using Information Technology to view, print, transmit, or create any offensive material including pornography; hate literature or any material that contravenes the VCH Respectful Workplace & Human Rights Policy is prohibited.

7. *Harassment*

   Using Information Technology or assets to create or transmit any material (by email, uploading, posting, or otherwise) that harasses another person is prohibited.

8. *Fraudulent and Unauthorized Commercial Activity*

   Using Information Technology or assets to make fraudulent offers or otherwise conducting unauthorized commercial activity in relation to selling or buying products, items, or Information Technology or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.

9. *Forgery or impersonation*

   Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information or using another person's email or other account to send messages or conduct activities without proper authorization is prohibited.

10. *Unsolicited email/Unsolicited bulk email (SPAM)*

Using Information Technology to create or transmit any unsolicited commercial email or unsolicited bulk email is prohibited. Activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk email, whether or not that email is commercial in nature, are prohibited.

11. Unauthorized access

Using Information Technology to access, or to attempt to access, the accounts of others, or to circumvent, or attempt to circumvent, security measures of VCH's or another entity's information or communications system is prohibited,

12. Collection of Personal Information

Using Information Technology or assets to collect Personal Information without their knowledge or consent is prohibited, unless authorized by applicable laws and VCH policies.

13. Reselling Information Technology

Reselling Information Technology, assets or services without VCH's authorization is prohibited.

14. *Unauthorized Software and Media*

Installing any non-standard VCH software, including copyrighted software for which VCH does not have an active license, is strictly prohibited. The downloading or storage of non-business related media (including movies, MP3's, image files) onto VCH/PHC technology and equipment is prohibited.

15. Disruptive and Unauthorized System or Network Activities

(a) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

(b) Causing security breaches or disruptions of network communication is prohibited. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(c) Port scanning or security scanning is expressly prohibited unless authorized by IMITS Security Services.

(d) Executing any form of network monitoring which will intercept data not intended for the Staff member is prohibited, unless this activity is a part of the employee's normal job/duty.

(e) Circumventing user authentication or security of any host, network or account is prohibited.

(f) Interfering with or denying service, without proper authorization, to any user is prohibited.

(g) Using any program/script/command or sending messages of any kind with the intent to interfere with or disable computer use via any means, without proper authorization, is prohibited.

Appendix 2: IMITS User Security Guidelines

Effective security is the responsibility of all VCH staff and other users. This guideline is designed to raise security awareness and enable staff and others to achieve security best practices. It is not intended to cover all aspects of Information Technology security, which are discussed in more detail in VCH security policies.

VCH believes that security is the responsibility of all Staff and other users of Information Technology. The security of Information Technology depends on the proper use of those resources. Security and other technologies may help to protect VCH resources and enforce company policies, but they will have little value if users are not aware of security best practices or attempt to circumvent them, whether intentionally or otherwise. For this reason, VCH strongly emphasizes the need for effective security practices by all individuals who are authorized to access its systems and resources, including Staff, partners and third-party service providers.

Recognize the importance of physical security:

VCH has clearly defined physical security controls in place at all VCH premises. Be aware of the controls and ensure that they remain intact. For example, do not block doors so that they remain open to the outside, and do not admit any unknown person to the premises without properly verifying his or her identity.

Be aware of your surroundings and the activity around you:

Many individuals (including employees, partners and third-party providers) are likely to be performing work on VCH premises at any given time. Some of these people are authorized to have access to sensitive systems and resources, or to specific areas of the premises, while others are not. If you believe someone is working in an inappropriate area or with an inappropriate resource — whether VCH staff or an outside party — you must inform your manager or supervisor.

Be on guard against "social engineering":

Technical security measures are improving rapidly, and for this reason, “social engineering” (fraudulent attempts to gain access to systems or information, often by telephone or e-mail) is becoming commonplace. For example: an unauthorized person may call, pretending to be a company employee who is experiencing a system failure and asking you to give a password or run a specific program. A request of this type is almost certainly fraudulent. Make certain that you know who you are talking to, and if you are in any doubt, contact IMITS Security Services.

Ensure that system maintenance is performed by authorized personnel only:

Maintenance personnel (either internal staff or third-party providers) may sometimes need privileged access to your systems or information resources. In most cases, you will be informed beforehand. If you are in any doubt about a request to access your system, contact your manager or the VCH Help Desk. Do not disclose your password to maintenance personnel under any circumstances.

Rely on VCH's IMITS personnel for service and support:

While it is often more convenient to ask your colleague next door, only the IMITS Staff is authorized and has the expertise to manage error correction and system configuration consistently throughout the organization. This also applies to software installations and workstation configurations.

Handle passwords with care:

Passwords are the most immediate and visible security measure, and you should handle them with at least the same care you would take with the keys to your home (see VCH Password Guidelines). Do not write them down — and certainly do not hide them under your keyboard or stick them on your monitor — and do not share them with anyone, even your closest colleagues. If you have any suspicion at all that your password may have become known to another person, change it immediately (see VCH Password Creation Guidelines).

Criticize security procedures if necessary, but do not circumvent them:

VCH recognizes that security controls may affect Staff's ability to do their jobs efficiently. If you believe that some security measures are too restrictive, discuss the issue with your manager or with IMITS Security Services. Do not simply try to circumvent the security measures that are causing problems for you.

Handle Confidential Information with due care at all times:

VCH's Confidential Information should be handled appropriately throughout the entire communications chain. For example, confidential documents should be printed only using printers that are in a physically secured location, printouts should be collected immediately, printed documents should be stored in locked cabinets, and documents that are no longer needed should be destroyed.

Follow the Rules in the IMITS List of Prohibited Activities:

Adhere to the rules prohibiting inappropriate activities using Information Technology as set out in the IMITS List of Prohibited Activities.

Ensure you are familiar with VCH policies:

Security threats are changing rapidly, and so are the measures VCH takes to combat them. For this reason, employees must exercise common sense and keep up to date with VCH's policies and procedures as they evolve to address new risks.

When in doubt, ask:

Effective security depends not only on technical, administrative and legal controls, but also on communication. If you have any questions or concerns about VCH's security policies, do not hesitate to contact your manager, the help desk or IMITS Security Services.