Appendix 4: HLI Acceptable Use Manual (attachment to Policy PR-0706)

Acceptable Use of Computer Systems

Version 1.1

Last updated: April 19, 2012

Policy

The UBC Centre for Heart Lung Innovation (HLI) systems and associated resources are provided to users to accomplish tasks related to and consistent with the HLI's mission. Access is provided to users to assist them to perform their work. Use of services such as network, e-mail or the Internet must not jeopardize or, delay operation of the system or the reputation and/or integrity of HLI.

Each user who is given access to HLI Centre systems must read the Centre for Heart Lung Innovation *Acceptable Use of Computer Accounts* Policy (PR-0706) and will sign an agreement stating that they have read and understood the terms and conditions of data and systems use.

Each user is responsible for ensuring that their use of all systems and data is appropriate and concordant with the acceptable use policy. The consequence of violating this policy may result in loss of privileges and discipline up to civil and criminal liability.

Definition

The term **Systems** applies to resources such as computer systems workstations, laptops, servers, printers, network, operating systems, applications and data and system software under the custody of the HLI.
The term **Users** applies to all persons authorized to access the HLI network and/or associated resources. This includes employees and non-employees (including but not limited to physicians, researchers, students, other trainees, and contractors).

Purpose

The purpose of this manual is to ensure that:

- Users are informed about acceptable and non-acceptable use.
- Disruption to services and activities is minimized.
- Users are educated about potential risks and liabilities associated with communications technologies and electronic data and systems.

TERMS AND CONDITIONS OF USE

Property

1. The HLI systems and associated resources are the property of the University of British Columbia.

Account Management

2. All potential users will be asked to read and sign an agreement to abide by the terms and conditions of use.
3. Access to an account will be provided, once the agreement has been signed.
4. The account will provide the user with access to the data and computing resources that are required to perform their duties.

Password Management

5. Centre for Heart Lung Innovation Policy PR-0705 addresses password management.
6. Users will be responsible for managing the confidentiality of their account password.
7. Inappropriate use of passwords would include, but is not limited to:
   - Revealing your password to another user.
   - Writing your password down and displaying it in an unsecured location.
   - Reusing your password for any other electronic logon
8. In order to minimize the risks associated with password confidentiality, user passwords should be non-obvious, hard-to-guess, confidential, and changed on a regular basis.

Security of Confidential Information

9. The Centre for Heart Lung Innovation Privacy Policy (PR-1001) addresses the users' responsibility to protect the confidentiality of information to which they have access.
10. Users who have access to electronic records, which contain personal information (e.g. patient records, employee records), must make every attempt to keep this information secure from unauthorized disclosure.
11. Workstations must not be left logged on when unattended and should be protected by key locks, passwords or other controls when not in use. Automatic password protected screen savers will be employed with timeout periods appropriate to the sensitivity of the data being accessed.
12. Computer monitors, printers, fax machines displaying personal information should be positioned out of public view.

Electronic mail and the Internet

13. Users must not use e-mail to distribute "confidential information" over un-trusted networks such as the Internet, unless the information is encrypted in accordance with HLI standards. There are significant differences between the security of e-mail sent within the internal network and e-mail sent via the Internet.
14. Users must not use e-mail systems such as AOL, Hotmail or local ISP websites to access HLI related e-mail. Access to such sites is considered high risk.
15. Users must not use e-mail and the Internet for activity considered misuse (See item 34).

For additional information contact Manager, IT Services.

Authorized Service Restrictions

16. Access to services such as e-mail and the Internet is a privilege that may be wholly or partially restricted without prior notice and without the consent of the user:
    - When required by and consistent with applicable law or policy;
    - When there is a reasonable suspicion that violations of policy or law have occurred or may occur; and,
    - When required to meet critical operational needs.

Monitoring and Disclosure

17. The Centre for Heart Lung Innovation reserves the right to have authorized personnel access any message, file, image or data created, sent or received by use of HLI systems for the purposes of determining whether there have been violations to its policy, breaches of security, or unauthorized actions on the part of an individual.
18. Users are reminded that audit trails are used to monitor access to messages files, and data each time they log-on to a computer workstation.
19. HLI may disclose information to law enforcement agencies without prior notice to the user.
20. In the course of their duties, IT staff may monitor use of user activity.

Responsibilities

21. **Users** are responsible for ensuring that their use of data, systems and associated computer services are appropriate and consistent with law and with the terms and conditions of use.
22. **Managers** are responsible for ensuring all users are made aware of the terms and conditions of use.

23. Managers are responsible for taking appropriate action when inappropriate use is suspected.
24. Managers are responsible for notifying the HR Manager, of staff transfers so that network accounts can be adjusted.
25. Managers are responsible for notifying the Manager, Human Resources of staff who are on temporary leave or who have been terminated.
26. The Manager of IT Services (or delegate), is responsible for monitoring network usage.

Content and Etiquette of Records

27. The language, tone, style and presentation of all records (e.g. such as e-mail and other correspondence) must conform to acceptable social and professional standards, including but not limited to the ***Human Rights Code*** and applicable policy on Workplace Discrimination and Harassment.
28. The creation of single topic messages should be done wherever possible to facilitate filing, retrieval and forwarding of information.

Blocking Internet Sites with Inappropriate Content

29. The Centre for Heart Lung Innovation has the right to utilize software that makes it possible to identify and block access to Internet sites containing material deemed inappropriate for the workplace.

Personal Use

30. The Centre for Heart Lung Innovation systems may be used sparingly for incidental personal use. This must not, however, detrimentally affect productivity, disrupt the system, harm the reputation of the HLI and/or be used for any activity considered misuse (See item 34). No personal computers or equipment may be connected to HLI Systems.

Electronic Record Creation, Storage, and Retention

31. Electronic files created and stored on the HLI Centre network are "records" as defined by the *Freedom of Information and Protection of Privacy Act (FOIPPA)*. E-mail records must comply with existing legislation including *FOIPPA* and the *Document Disposal Act*. The intentional alteration or destruction of a record for the purpose of evading an access request is an offense under *FOIPPA*.
32. The use, management and retention of e-mail records which include personal information must be guided by principles of confidentiality, protection of privacy and

best practices. Be certain of the recipient and address to which the information is to be sent.

33. Each user will be allocated limited storage space for accounts such as e-mail, e-drives, and voice mail. It is the responsibility of each user to manage their accounts within these limitations.

Misuse

34. Centre for Heart Lung Innovation systems and data must **not** be used for:

- Illegal, unethical, or immoral uses. Illegal use may include, but is not limited to: obscenity, child pornography, threats, harassment, theft, violation of copyright law;
- Sending offensive, objectionable, abusive, pornographic, obscene, sexist, racist, or harassing messages, images or other materials, including adult-oriented Web sites or news groups;
- Sending defamatory, derogatory, slanderous, or false messages;
- Leaking confidential information;
- Political activities (such as expressing political opinion and organizing political rallies);
- Distribution of union communication for purposes contrary to the interest and operation of the organization, including but not limited to, organizing rallies, defamatory remarks about the Employer, encouraging job action, or any activity not considered day-to-day activity in the course of Employer/Union business
- Unauthorized access to other users' accounts, (e.g. e-mail, voice mail), or to any otherwise unauthorized data;
- Transmission or downloading that infringes copyright or other intellectual property rights;
- Accessing audio (e.g. music), video, games, game sites, or movies for personal use (these activities excessively consume network capacity);
- Using Internet Chat rooms, Bulletin Boards, or list servers for other than work related business;
- Downloading large non-work related files, such as software, screen savers, and movie or music files;
- Conducting or pursuing one's own business interests or other activities for personal financial gain;
- Attempting to obscure the origin of any message or downloading any material under an assumed identity or Internet address;
- Uses that may compromise system integrity or degrade system performance, for example:

- Sending or forwarding chain letters;
- "Spamming", that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail;
- "Letter-bombing", that is, to re-send the same e-mail repeatedly to one or more recipients;
- Sending hoaxes; and,
- Sending unauthorized advertisements or notices.

Copyright

35. Dissemination of copyrighted materials using the HLI's e-mail system is prohibited. Dissemination without the appropriate authority or approvals may result in liability under the *Copyright Act*.
36. Duplication of purchased or developed software for use in connection with personal computers without obtaining proper authorization is prohibited. Infringement claims under the *Copyright Act* can arise from such activities as copying graphics for wallpapers or screen savers, making unauthorized copies of software or loading unauthorized copies of personal software onto HLI computers.

Consequences

37. Inappropriate use of HLI systems and associated resources may lead to loss of network access privileges and discipline up to and including immediate termination of employment/contract/association with the HLI.
38. Failure to follow the law may lead to civil and/or criminal penalties.

Associated Documents

Centre for Heart Lung Innovation Policies:

- PR-0705: Password Policy;
- PR-0706: Acceptable Use of Computer Accounts;
- *Agreement to abide by the Centre for Heart Lung Innovation policy concerning acceptable use of IT resources*.

UBC Policy #104: Responsible Use of Information Technology Facilities and Services (http://www.universitycounsel.ubc.ca/policies/policy104.pdf)

References

1. AHIMA. *Email Security*. Dec. 1996
2. AHIMA. *Practice Brief*. Email Security. June 1997

3. Alberta Cancer Board. *Computer System Usage Policy*. F2-4. January 2002.
4. CIO Information Bulletin. Chief Information Officer for the Province of BC. *Creating and Using Computer Passwords*. February 2002.
5. CIO Information Bulletin. Chief Information Officer for the Province of BC. *Using the Government Computer Network Responsibly*. January 2001.
6. *Criminal Code of Canada*. Section 301.2. Section 387 (1.1).
7. EPTW. *Terms and Conditions of Employment*. 8.11.1 E-mail, Internet and Computer Use. P.8-88.1 – 8-88.24.
8. FOIP Bulletin. Freedom of Information and Privacy Protection. *E-mail: Access and Privacy Considerations*. December 2001.
9. Freedman, Bradley. *Communications System Policies – Part 11: Creating a Communications System Policy*. HCIM&C 4th Quarter. 1998. P.40-42.
10. HEABC. Policy 4.2.8 *Electronic Mail Usage*. June 2001.
11. HEABC. Policy 4.2.9 *Internet Usage*. June 2001.
12. McGill Computing Facilities. *Code of Conduct for Users*. (http://www.mcgill.ca/ncs/policies/).
13. Ministry of Management Services. *Creation, Retention and Destruction of Email Records and FOI Access Policy*. Jan. 1996
14. Ministry of Management Services. *Educational Proposal for E-mail Management and Systems*. Jan. 1996
15. Ministry of Management Services. Freedom of Information and Protection of Privacy Branch. *Transitory Records*. FOIPP Provisions. (www.mser.gov.bc.ca).
16. Office of the Information and Privacy Commissioner of BC. *Policy on Confidentiality of E-mail at the Office of the Information and Privacy Commissioner*. February 1997.
17. Office of the Information and Privacy Commissioner of Ontario. *Privacy Protection Principles for Voice Mail Systems*. March 1996.
18. Smith, Brock. *Avoiding Liability for E-mail and Internet Misuse*. HCIM&C 4th Quarter 1999. P.32-33.
19. Vancouver General Hospital. Policy AD0400. *Electronic Mail Usage*. October 1999.
20. Vancouver General Hospital. Policy AD0500. *Internet/Intranet Usage*. March 1999.
21. *Interior Health Authority Acceptable Use* policy,
22. Children's and Women's Hospital AK 0040 – Communications Systems, Use of
23. Provincial Health Services Authority Acceptable Use policies, Interior Health Authority Acceptable use policies