Covenant Health	**Information Technology Acceptable Use and Safeguards**	**Corporate Policy & Procedures Manual**
		Number: X-50
		Date Approved May 12, 2014
Approved by: President and Chief Executive Officer		**Date Effective** July 11, 2014
		Next Review (3 years from Effective Date) July 2017

Purpose

To provide direction for appropriate use of information technology resources within Covenant Health facilities or by remote access and to establish safeguards and controls to protect the security of the resources.

Policy Statement

Information technology resources are provided for work related purposes. Users must comply with administrative, technical and physical safeguards to protect Covenant Health's information technology resources as well as the information held on those resources.

Applicability

This policy applies to all Covenant Health facilities, staff, physicians, volunteers, students and any other persons acting on behalf of Covenant Health (personnel).

Responsibility

All personnel are responsible to take precautions to ensure personal information, health information and other information held in our information systems is protected from unauthorized access or disclosure, security threats, and environmental hazards.

Principles

The use of information technology resources shall be consistent with the mission, vision, values and operational objectives of Covenant Health in the provision of patient care, support services and related business activities.

Covenant Health relies on Alberta Health Services (AHS) as our primary service provider for information technology infrastructure, hardware, software and related support functions and collaborates with the AHS Information Technology Security & Compliance Team to ensure that information systems security standards and safeguards are in place to protect information technology resources.

Procedure

1. General Use of Information Technology Resources

1.1. Information technology resources are provided for the primary purpose of facilitating Covenant Health's health services operations and business related activities. While reasonable use for personal purposes is permitted, information technology resources shall not be used to conduct personal business matters or for private financial gain.

1.2. Covenant Health owns all electronic transactions undertaken on Covenant Health information technology resources, including mobile devices and wireless communication devices, and these shall be subject to all applicable legislation and Covenant Health policies and standards.

1.3. Users shall not interfere with or disrupt information technology resources or other users through actions including, but not limited to, the propagation of computer viruses, the disconnection of, or damage to equipment and services.

1.4. The use of information technology resources to gain or attempt to gain unauthorized access to information, services, or other information technology resources within or outside Covenant Health is strictly prohibited.

1.5. Users should not have any expectation of privacy regarding their communications, transmissions or other use of information technology resources. Use of information systems is monitored and audit logs and reports may be reviewed at any time to identify potential unauthorized access to personal or health information not required by the user to perform his or her job duties. Covenant Health reserves the right to review or block a user's use of the resources assigned to them.

2. Internet

2.1. Reasonable personal use of the internet during break periods is permitted provided such use does not conflict with legislation or other Covenant Health policies and does not impact Covenant Health's operational requirements.

2.2. Using services such as electronic chat, instant messaging, streaming audio/video, photo/video sharing websites, websites offering cloud based services and other similar programs for personal purposes is prohibited.

2.3. Users are prohibited from accessing, distributing, downloading, recording, or transferring any form of internet or other materials which are pornographic, obscene, abusive, discriminatory, sexually harassing, defamatory, libelous or otherwise offensive.

3. Email Use

3.1. Each email user is provided with a unique email account that must not be shared.

3.2. All transmissions of personal or health information to email addresses external to the Covenant Health/AHS secure network must be encrypted. Instructions for encrypting email can be obtained on the AHS intranet at http://insite.albertahealthservices.ca/3141.asp or by contacting the IT Service Desk.

3.3. Automatic email forwarding to sites outside of Covenant Health or to non-Covenant Health devices is restricted to those approved by Information Technology.

3.4. Email messages containing any information subject to a copyright must include the appropriate copyright information.

3.5. Encryption software, digital certificates or secure protocols shall be used as required to protect email messages.

3.6. Covenant Health reserves the right to access a user's email records. Disclosure of email records to third parties may be required in accordance with applicable information and privacy legislation.

3.7. The use of email to forge or attempt to forge email messages, to send large attachments without a proper business function, to send illegal / harassing / objectionable / threatening email messages, to transmit unsolicited information to individuals without an authorized business function, or to send commercial advertisements or chain letters is prohibited.

3.8. Users shall not open attachments sent by unknown or suspicious parties or create/modify/execute/transmit any computer program or instructions intended to obscure the true identity of an email sender.

4. Software Use

4.1. Users shall not, under any circumstances, independently install or download any software on to a Covenant Health information technology resource.

4.2. Requests for new or additional software should be sent to the I.T. Service Desk or a supervisor. A supervisor's formal approval based on business need may be required to obtain the requested software. AHS Information Technology will assist as required to obtain and install the software.

5. Information Technology Resources Safeguards

5.1. All information technology security safeguards and standards set out and communicated by Alberta Health Services, as Covenant Health's information technology service provider, must be adopted by all information systems users and other individuals acting on behalf of Covenant Health.

5.2. All staff and other individuals acting on behalf of Covenant Health shall adhere to the security requirements and safeguards outlined in the attached appendices:

- Appendix A – Physical Safeguards for Security of Information Technology Resources
- Appendix B – Administrative Safeguards for Security of Information Technology Resources
- Appendix C –Technical Safeguards for Security of Information Technology Resources

Definitions

Access privileges means privileges granted to an individual for access to or use of Covenant Health information technology resources to perform tasks assigned to the individual. Privileges may be granted for access to physical or electronic resources.

Information technology resource means any device or system owned or provided by Covenant Health/AHS used to generate, process, transmit, communicate, store, or access information, including but not limited to information technology infrastructure, systems, hardware, software, networks, shared drives, computer equipment and devices, the Internet, email, databases, applications, mobile computing devices and mobile storage devices.

Mobile computing device means a portable electronic device such as notebook computers, laptops, tablets, text pagers, smart phones, and other similar devices.

Mobile storage device means a portable device used to store data or information, such as analog or digital voice recorders, external hard drives, memory cards, flash storage drives, optical storage devices (eg. CDs, DVDs, and Blu-ray discs), and other similar devices.

Health Information means any recorded information that relates to an identifiable individual and is collected during the provision of a health service to the individual such as:

- demographics, registration, residency, health service eligibility or billing information
- diagnostic, treatment and care information

Personal Information means recorded information, not including health information, about an identifiable individual including, but not limited to, name, home address or contact information, race, ethnic origin, gender, marital status, educational/ financial/ employment/criminal history, and opinions of others about the individual.

Security means employing methods to guard or protect information technology resources against misuse, theft, or other dangers, safeguarding the information held on the resources from unauthorized access or disclosure.

User means an individual who uses any information technology resource.

Related Documents

Corporate Policies:

- X-10, Confidentiality Agreement and Privacy Training
- X-25. Contractor Requirements for Security of Information and IT Resources
- X-40, Information Privacy Breach or Information Systems Security Incident Response
- X-45, Information Security Classification
- X-55, Privacy Impact Assessments and Monitoring
- X-60, Transmission of Personal or Health Information
- X-65, Transportation of Personal or Health Information
- I-35, Identification Cards

Caritas Health Group Policy #V-C-25, *Key and Lock Control*

Information and Privacy Resources http://www.compassionnet.ca/Page1507.aspx

References

Freedom of Information and Protection of Privacy Act
FOIP Guidelines and Practices, 2009
http://www.servicealberta.gov.ab.ca/foip/resources/guidelines-and-practices.cfm

Health Information Act
HIA Guidelines and Practices Manual, March 2011
http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf

Revisions

N/A

APPENDIX A

Physical Safeguards for Security of Information Technology Resources

Information technology equipment, mobile or fixed, shall be secured utilizing the highest level of safeguard that can be employed to protect the equipment and/or the information that may be accessed, while ensuring that operational needs are met.

For example:

- Equipment will be located in an area with a defined security perimeter or barrier with entry controls (eg. key locks, swipe card access, alarms, staffed reception desks).
- Equipment will be protected from unauthorized removal with security cables, cabinetry or other locking devices whenever possible.
- In areas accessible to the public, a privacy screen should be used or a monitor positioned to prevent unauthorized viewing of confidential information.
- Mobile devices must be kept in a user's possession at all times or stored in a secure lockable location out of sight when not in use.

APPENDIX B

Administrative Safeguards for Security of Information Technology Resources

1. Confidentiality and user agreement
   - Users shall sign the necessary confidentiality and user agreements indicating they have read, understood and agree to comply with Covenant Health policies and privacy and security standards.
2. Education and training
   - Users will be informed of their information technology responsibilities by their immediate supervisor upon appointment.
   - Users shall complete relevant privacy and security training sessions as required.
3. Identification cards
   - Individuals wishing to access information technology resources or equipment should ensure that their identification is clearly visible at all times.
   - When it is not possible for identification to be clearly visible, the individual must produce his/her Covenant Health identification upon request.
4. Reporting threats
   - Any knowledge or suspicion of a threat to the integrity of a user ID/password, information system or information technology resource shall be immediately reported to the Alberta Health Services Information Systems Security and Compliance Team at SecurityIncident@albertahealthservices.ca.

APPENDIX C

Technical Safeguards for Security of Information Technology Resources

1. User access and termination procedures for network access, information systems applications, internal networks, shared file drives
   - Any individual requiring access to an information technology resource, system or application, will use the formal user registration procedure to apply for access.
   - Users shall be assigned a unique user ID which will limit access to the level required to perform role related responsibilities.
   - Requests for user access must be approved by the individual's immediate supervisor.
   - Immediate supervisors are responsible to submit requests for termination of, or changes to, user access privileges in a timely fashion upon transfer or termination of an individual's employment, agreement, contract or appointment.

2. User IDs, Passwords and logging off
   - User IDs and passwords shall not be shared or transferred for use by any user.
   - Users are responsible to safeguard their passwords and shall take necessary security precautions to prevent any user ID misuse.
   - Users must log off or lock their computer when stepping away from their workstation.
   - Users are responsible for all actions performed while their user ID is in use.
   - If it is suspected that user credentials have been lost or compromised, the AHS Information Technology Service Desk must be notified.

3. Mobile Devices
   - Users shall not use automatic log-in procedures (eg. automatic password saving).
   - All mobile devices shall be password controlled and utilize approved data encryption.

4. Virus Protection and Patch Updates
   - All computing devices connecting to the COV/AHS network must use a standard approved antivirus product.
   - Users should reboot their computers at least once per week to ensure virus protection and patch updates.

5. Storage of personal or health information
   - No individually identifying information may be stored on a computer's hard drive.
   - Individually identifying information stored on a network drive must be placed in secure folders where access is limited only to users who require the information in order to perform their job duties.
   - Mobile devices or external storage drives used to store individually identifying information shall be encrypted according to AHS I.T. standards.

6. Audit and monitoring
   - Information systems usage by staff or other individuals acting on behalf of Covenant Health may be monitored at any time to reduce risks of human error, fraud or misuse of information.
   - Processes shall be established to conduct periodic, regular or ad hoc audits of information systems to ensure that access to information complies with applicable legislation and Covenant Health policies.