PURPOSE

• To set out acceptable use of Alberta Health Services’ (“AHS”) Information Technology Resources (“IT Resources”).

• To maintain the integrity and security of AHS IT Resources.

• To comply with applicable legislation

POLICY STATEMENT

The IT Resources of AHS, including access to the Internet and electronic forms of communication (e.g. email), are primarily intended for AHS business purposes. Users utilizing AHS IT Resources shall comply with the AHS Code of Conduct, and applicable AHS policies and procedures including, but not limited to, those related to User-IDs, passwords, email, information security, privacy, and confidentiality.

Users, as representatives of AHS, shall exercise careful judgment when using the Internet, intranet, email, or other AHS IT Resources. The use of IT Resources and the content of email and other forms of communication may be audited or monitored, at the sole discretion of AHS without notice to Users.

APPLICABILITY

Compliance with this policy is required by all AHS employees, members of the medical and midwifery staffs, students, volunteers, and other persons acting on behalf of AHS (including contracted services providers as necessary). This policy is subject to all applicable laws.
POLICY ELEMENTS

1. **General Computing**
   1.1 AHS Information Technology may at any time monitor, without notification to the User, all assigned User accounts and activities.
   
   1.2 Users shall:
      a) each be assigned a unique User-ID to access AHS IT Resources;
      b) be responsible for all actions taken by that User-ID;
      c) take necessary security precautions (e.g. protecting access to workstations) to prevent any User-ID and/or password misuse; and
      d) not allow another individual to use their User-ID and/or password.
   
   1.3 Users shall not remove or tamper with any IT Resources, including hardware or software.
   
   1.4 AHS IT Resources shall not be used to conduct activities for private financial gain.
   
   1.5 Users shall only access the minimum information necessary for the performance of their duties with AHS.
   
   1.6 Users are prohibited from accessing or distributing illegal or objectionable material, including but not limited to:
      a) obscene or pornographic material;
      b) hate propaganda or discriminatory material;
      c) defamatory and libellous material; and
      d) sexually harassing material.
   
   1.7 Copyrighted materials (such as third-party software) shall only be copied with a proper license or expressed written permission from the software manufacturer.

2. **Electronic Communications**
   
   2.1 AHS owns all electronic communications, including those to social media sites, transmitted over AHS-owned IT Resources Users shall have no expectation of confidentiality regarding their electronic communications. AHS may access, monitor, block, and review these communications in accordance with applicable legislation.
   
   2.2 Electronic communications shall be subject to all applicable legislation and AHS Secure Program Standards.
   
   2.3 Electronic communications containing any copyrighted information must include the appropriate citations and acknowledgement of copyright. Any copyrighted information must be used in accordance with applicable legislation.
2.4 Users shall not:

a) forge or attempt to forge email messages;
b) send or forward large attachments without a proper business function;
c) send illegal, harassing, objectionable, or threatening email messages;
d) transmit unsolicited information to multiple individuals unless it is for an authorized business function;
e) open attachments sent by unknown or suspicious parties;
f) send commercial advertisements or chain letters; or
g) create, modify, execute or transmit any computer program or instructions intended to obscure the true identity of an email sender.

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

2.6 AHS electronic group mailing lists (i.e. lists allowing distribution of email messages to multiple recipients using a single address) shall be used for AHS business only. All group mailing lists shall have designated owners responsible for ensuring list-member accuracy.

2.7 Automatic email forwarding to sites outside of AHS is restricted to those approved by AHS Information Technology.

3. Information Security

3.1 All electronic transmissions of Records, including Personal or Health Information, shall be in compliance with the Freedom of Information and Protection of Privacy Act (Alberta), the Health Information Act (Alberta), and applicable AHS Information and Technology Management policies and AHS IT Security and Compliance Program Standards.

3.2 Transmission of information via email within the AHS-secured internal network shall occur only when there is a direct connection to the purpose for which the information was originally collected.

3.3 Transmission of Personal Information and identifiable Health Information by email to an external email account shall only occur if the information is encrypted and the recipient can be authenticated in accordance with the Transmission of Information by Facsimile and Electronic Mail policy (#1113).

3.4 Transmission of Personal Information and Health Information via file transfer process shall only be through the secure AHS-implemented file transfer process.

4. Internet and Software Use

4.1 Reasonable personal use of AHS internet is permitted provided such use does not impact upon AHS' operational requirements and is in accordance with applicable...
legislation, the principles of the AHS Code of Conduct, and applicable AHS policies and procedures.

4.2 AHS Internet shall not be used to conduct personal activities for private financial gain.

4.3 Accessing and using social media sites on AHS IT Resources for business purposes is permitted in accordance with the AHS Social Media policy (#1139).

4.4 Users shall not access or distribute illegal or objectionable internet material, including but not limited to:

   a) obscene or pornographic material;
   b) hate propaganda or discriminatory material;
   c) defamatory and libellous material; and
   d) sexually harassing material.

4.5 Users shall not, under any circumstances, personally install or download any software onto an AHS IT Resource. Users shall contact AHS Information Technology when additional software is required. Approval of requests for additional software shall be based on business needs.

4.6 AHS Information Technology shall monitor and assess risks posed to AHS by the use of the Internet and will disable access to any site/platform where there is reason to believe AHS systems or data are at substantial risk.

5. **IT Security & Compliance**

5.1 AHS shall make all reasonable efforts to protect its IT Resources from tampering, unauthorized access, and loss. Users shall comply with AHS Information and Technology Management policies and AHS IT Security and Compliance Program Standards to ensure the protection and security of AHS information and IT Resources.

5.2 Appropriate permission or authorization shall be required for Users to access password protected or encrypted information.

5.3 Users shall not interfere with or disrupt IT Resources or other Users, through actions including, but not limited to, the propagation of computer viruses, the disconnection or damage to equipment and services or other malicious activities.

5.4 Use of IT Resources to gain or attempt to gain unauthorized access to information, services, or other resources within or outside AHS is strictly prohibited.

6. **Mobile Computing Devices and Mobile Storage Devices**

6.1 Users shall be responsible for the security and protection of AHS information and IT Resources in their possession. To minimize the risk of theft of Mobile Computing...
Devices and Mobile Storage Devices and the information carried therein, Users shall:

a) use locking mechanisms for Mobile Computing Devices and Mobile Storage Devices whenever possible;

b) ensure that Mobile Computing Devices and Mobile Storage Devices remain in the User’s possession at all times, in accordance with the AHS IT Security and Compliance Program Standards; and

c) not use automatic log-in procedures (e.g. automatic password saving).

d) store them in a secure location out of sight (e.g. in a locked file drawer) when not in use.

6.2 All Mobile Computing Devices and Mobile Storage Devices must use AHS-approved encryption standards to ensure the confidentiality and integrity of the stored information.

7. Compliance
Use of AHS IT Resources constitutes acceptance of compliance responsibilities identified in agreements signed upon appointment and applicable AHS policies. Failure to abide by the agreement and applicable AHS policies or using AHS IT Resources inappropriately shall be grounds for disciplinary action up to and including dismissal. Where illegal activities have occurred, the appropriate authorities shall be notified.

DEFINITIONS

IT Resource means any AHS-owned or controlled asset used to generate, process, transmit, store, or access AHS information, which includes but is not limited to IT infrastructure, computer facilities, systems, hardware, software, information systems, networks, shared drives, computer equipment and devices, Internet, email, databases, applications, Mobile Computing Devices, and Mobile Storage Devices.

Mobile Computing Device means portable electronic devices including but not limited to Portable Digital Assistants (PDAs), notebook computers, laptops, desktop PCs, Palm Pilots, Pocket PCs, Blackberrys, tablets, text pagers, “smart” phones, and other similar devices.

Mobile Storage Device means portable devices used to store data including but not limited to analog or digital voice recorders, external hard drives, memory cards, flash and other data storage drives, optical storage devices (e.g. CDs, DVDs, and Blu-ray discs), regular cell phones, and other similar devices.

Record means documents, data or information of any kind, in any medium (e.g., paper, digital, and audio-visual media), and in any format (e.g. documents, spread sheets, databases, emails, blogs, wikis, and website pages) created, received, recorded, and maintained by Alberta Health Services as part of its services or business. This definition includes health Records, but does not include computer software or any mechanisms that produce Records.

If you have any questions or comments regarding the information in this policy, please contact the Corporate Policy Department at corporatepolicy@albertahealthservices.ca. The Corporate Policy website is the official source of current approved corporate policies, procedures, and directives.
Security means the guarding or guaranteeing of the safety of AHS information and IT Resources against misuse, theft or other dangers, and protecting the privacy and maintaining the integrity of information.

User means any person who accesses or uses an AHS IT Resource.

REFERENCES
• Appendix “A” – Code of Behaviour for Computer Use
• AHS Code of Conduct
• AHS Policies and Procedures:
  o Access to Information (Physical, Electronic, Remote) (#1105)
  o Contractor Requirements for Security of Information and Information Technology Resources (#1107)
  o Collection, Access, Use, and Disclosure of Information (#1112)
  o Delegation of Authority and Responsibilities for Compliance with FOIPP and the HIA (#1108)
  o Information Security and Privacy Safeguards (#1143)
  o Records Destruction (#1133-02)
  o Records Management (#1133)
  o Records Retention Schedule (#1133-01)
  o Safe Disclosure/Whistleblower (#1101)
  o Transitory Records (#1133-03)
  o Transmission of Information by Facsimile and Electronic Mail (#1113)
• AHS IT Security and Compliance Program Standards
• Freedom of Information and Protection of Privacy Act (Alberta)
• Health Information Act (Alberta)

REVISIONS
January 10, 2012

If you have any questions or comments regarding the information in this policy, please contact the Corporate Policy Department at corporatepolicy@albertahealthservices.ca. The Corporate Policy website is the official source of current approved corporate policies, procedures, and directives.
APPENDIX “A”

CODE OF BEHAVIOUR FOR COMPUTER USE

1. **Personal Responsibility and Accountability**
   All Users shall be personally responsible and accountable for all activities undertaken under their assigned credentials/User-ID. Where it is suspected that credentials/User-ID are lost or compromised, Users shall immediately notify the AHS IT Service Desk for assistance and direction. The Service Desk staff is required to report the matter to IT Security and Compliance for investigation.

2. **Access to IT Resources**
   Explicit authorization is required for access to AHS’ IT Resources. Unauthorized use of AHS' IT Resources, or use of false or misleading information to gain use of these resources, is strictly prohibited. AHS IT Resources shall not be used to gain unauthorized access to other individuals’, organizations’, or institutions’ computing facilities and technology.

3. **Usage of IT Resources**
   AHS’ IT Resources are primarily intended for AHS business purposes. Using AHS’ IT Resources to conduct activities for private financial gain is not permitted. Additionally, Users must not:
   - permanently or temporarily alter or interfere with the standard configuration, operation, or procedures related to AHS IT Resources through personally installing or downloading software onto an AHS IT Resource; and
   - negatively impact the operational requirements of AHS or alter the performance of AHS computer networks and/or connected devices.

4. **Sharing of Passwords or User-IDs**
   Sharing of passwords or allowing other individuals to use a Users’ unique User-IDs is prohibited. Users shall take reasonable precautions to protect the privileges assigned to them and ensure terminals or workstations are logged-off when left unattended or not in use.

5. **Software Piracy and Use**
   Users shall ensure software is legally copied and used in accordance with its license.

6. **Regular Computer Reboots**
   Computing devices connecting to AHS networks must use a standard anti-virus product approved by the AHS IT Security and Compliance Office. It is strongly recommended that Users reboot a minimum of once per week to ensure virus protection and patch updates.

7. **Use of AHS Email Accounts**
   Email is a corporate resource. AHS owns all email transmissions on AHS networks and shall monitor email accounts as required. Users’ emails are not private and users should not expect that their emails are private. Email transmissions may be subject to public disclosure in accordance with applicable legislation. All electronic transmissions (including, but not
limited to emails, texts, and transmissions to social media sites) of AHS information shall be in accordance with applicable legislation and AHS policies.

8. Need to Know
Users shall access the minimum information necessary through AHS IT Resources to fulfill their duties on behalf of AHS, and shall only share the minimum information necessary through IT Resources with colleagues or other staff as necessary to fulfill their AHS-related duties. Users shall only access information or records through IT Resources as required to fulfill their AHS duties. Users shall only access patient and Health Information through IT Resources where:

   a) they are on the patient’s treatment team; or
   b) it is required in the course of their duties.

9. Protection and Privacy of Information
Users shall maintain and protect the confidentiality of any and all information accessed through the use of AHS IT Resources. Users shall take steps to safeguard against unauthorized access, as well as report improper activities.

10. Storage of Electronic Information
All AHS electronic information is owned by AHS and shall be stored on AHS protected network drives which have proper access controls to ensure only authorized access. Storing AHS electronic information on workstations or memory devices and electronic devices is not permitted unless specifically authorized by IT Security and Compliance and the information is encrypted according to AHS Secure Program Standards.

11. Reporting Improper Activities
Users must immediately report improper activities or any activity which is perceived to be improper on AHS IT Resources to the AHS IT Service Desk. The Service Desk staff shall report the matter to IT Security and Compliance for investigation. Improper activities, or activities which are perceived to be improper that involve information, shall be reported to the AHS Information & Privacy Office.