Alberta Health Services

POLICY

TITLE

CONTRACTOR REQUIREMENTS FOR SECURITY AND PRIVACY OF INFORMATION AND INFORMATION TECHNOLOGY RESOURCES

SCOPE
Provincial

DOCUMENT #
1107

APPROVAL AUTHORITY
Corporate Services Executive Committee

INITIAL EFFECTIVE DATE
June 24, 2009

SPONSOR
Legal & Privacy / Information Technology

REVISION EFFECTIVE DATE
October 16, 2019

PARENT DOCUMENT TITLE, TYPE AND NUMBER
Not applicable

SCHEDULED REVIEW DATE
October 16, 2022

NOTE: The first appearance of terms in bold in the body of this document (except titles) are defined terms – please refer to the Definitions section.

If you have any questions or comments regarding the information in this document, please contact the Policy & Forms Department at policy@ahs.ca. The Policy & Forms website is the official source of current approved policies, procedures, directives, standards, protocols and guidelines.

OBJECTIVES

- To outline to **contractors** and individuals negotiating, administering, or managing contracts on behalf of Alberta Health Services (AHS) the **security** requirements for using, accessing, or provisioning AHS information or **information technology (IT) resources**.
- To comply with *the Freedom of Information and Protection of Privacy Act* (Alberta) (FOIP) and the *Health Information Act* (Alberta) (HIA).
- To support the expected InfoCare behaviours of **AHS people**.

PRINCIPLES

Contractors using, accessing, or provisioning of AHS information or IT resources (e.g., third party service providers) shall implement and maintain controls for the security of information and IT resources and comply with applicable AHS policies, procedures, and standards.

Individuals negotiating, administering, or managing AHS contracts shall ensure contractors comply with this and other applicable AHS policies, procedures, standards, and with the terms, such as information management, specified in applicable contracts.

Prior to establishing a contractual relationship, AHS shall evaluate contractors for potential security risks. Contracts or agreements, which may specify additional security requirements, shall be completed and signed before a contractor is granted privileges for access to, or provisioning of, AHS information or IT resources.

APPLICABILITY

Compliance with this document is required by all Alberta Health Services employees, members of the medical and midwifery staffs, Students, Volunteers, and other persons acting on behalf of Alberta Health Services (including contracted service providers as necessary).

ELEMENTS

1. Contractor Overall Security Responsibilities

1.1 Security Infrastructure

a) Contractors shall ensure security controls are implemented and maintained. Contractors shall set out the roles and responsibilities of its staff with responsibility for information management and Information Risk Management, and maintain a current list of staff responsible for the implementation of security policies, procedures, practices, and standards.

1.2 Monitoring

a) AHS Information Technology may monitor a contractor to ensure compliance with applicable AHS policies, procedures, and standards. Monitoring may include, but is not limited to, ongoing or random security audits.

1.3 Annual Review and Audit

a) Information Risk Management may require a contractor to conduct an annual review and/or an annual technical audit of its security policies, procedures, practices, and standards. Any identified security gaps or areas of non-compliance shall be clearly documented.

b) Completed reviews and/or technical audits shall be submitted to the Information Risk Management within seven (7) days of completion. Information Risk Management shall prepare a final report, including recommendations for remedying deficiencies where appropriate, and forward the report to the contractor and applicable AHS people and committees.

c) Where Information Risk Management identifies deficiencies, contractors shall have thirty (30) calendar days to implement remedies and notify the Information Risk Management that such deficiencies have been addressed. Contractors failing to remedy the identified deficiencies shall be penalized in accordance with the provisions of their specific contracts.

1.4 Privacy Impact Assessments

a) The AHS Information & Privacy Department shall determine whether the goods and services performed by the contractor require a **Privacy Impact Assessment** (PIA) in accordance with the *Privacy Impact Assessments* Policy. Contractors shall be notified as necessary, and shall participate, cooperate, and comply with the AHS PIA process.

1.5 Disaster Recovery Plan

a) Contractors shall, as specified in a contract or on the request of Information Risk Management, prepare and submit disaster recovery and/or business continuity plans to ensure ongoing protection of access to or provisioning of AHS information and IT resources in the event of a disaster or disruption in normal business operations.

2. Access to AHS Information and IT Resources

2.1 Contractor Access Review

a) The AHS Information & Privacy Department or Information Risk Management shall identify and document deficiencies and risks associated with a contractor's access to AHS information or IT resources through an initial access review. Contractors may be requested to perform a full security review as a result of an access review.

2.2 Access Privileges

a) Individuals negotiating, administering, or managing AHS contracts, in conjunction with Information Risk Management, Information & Privacy Department, and/or Protective Services (or **facility designate**) as appropriate, shall evaluate contractors to determine the appropriate **access privileges** for contractors. Contractor access privileges, including remote access, shall be granted in accordance with the *Access to Information (Physical, Electronic, Remote)* Policy.

b) Contractors shall not receive access privileges until:

(i) the contractor has signed an approved contract with AHS;

(ii) the contractor has completed designated pre-requirements set out in the contract; and

(iii) identified deficiencies have been corrected to the satisfaction of Information Risk Management and Information & Privacy Department.

c) Contractors shall request and receive approval before granting access privileges to other individuals or organizations. Contractors may be

required by Information Risk Management to perform a security review prior to the contractor granting any access privileges to other individuals or organizations.

d) Where contractors have approval to grant access privileges to other individuals or organizations, the access shall be for the minimum information necessary to fulfil their responsibilities on behalf of AHS. The contractor shall inform the access recipients of their responsibility to comply with applicable AHS policies while exercising their granted access rights.

2.3 Contract or Agreement Expiration or Termination

a) Immediately upon expiration or termination of a contractor's agreement or contract with AHS, all access privileges shall be revoked, and AHS information and IT resources returned.

3. Contractor Human Resource Requirements

3.1 Contractors shall have human resource processes and practices in place to maintain the security and integrity of AHS information and IT resources.

3.2 Contractors shall ensure that:

a) an employment screening process, including reference verification, is implemented and complied with;

b) all employment agreements and job descriptions contain confidentiality requirements during and upon termination of employment, including specific penalties or disciplinary action for intentional, accidental, or unintentional **information security incidents** or loss or damage to AHS information or IT resources; and

c) policies are implemented requiring staff or representatives of the contractor to comply with generally accepted principles for computing use, applicable AHS policies and procedures, and clearly defined information and IT resource management processes.

3.3 Contractors, individual or firms, shall ensure staff who have or will have access to AHS information or IT resources:

a) are familiar with, understand, and agree to comply with all applicable AHS policies, procedures, and standards;

b) receive appropriate privacy and security awareness training consistent with AHS training practices;

c) visibly display an identification badge clearly indicating the individual is acting on behalf of the contractor, while working in AHS facilities;

d) sign and agree to comply with the terms of a confidentiality agreement and user agreement; and

e) receive suitable supervision during job training to ensure the security of AHS information and IT resources are protected and maintained.

4. Information Security

4.1 Contractors shall have mechanisms and comply with applicable AHS policies processes to ensure AHS information and IT resources are managed in compliance with AHS policies, procedures, and standards.

4.2 Retention, Destruction, and Disposal

a) Contractors shall ensure that retention, destruction, and disposal of AHS information and IT resources are in accordance with the AHS *Records Retention* Schedule, *Official Records Destruction* Procedure, and other AHS policies, procedures, and standards.

4.3 Classification and Inventory

a) All information generated by contractors and or IT resources acquired on behalf of AHS shall be classified and inventoried by contractors. Contractors shall:

(i) maintain and review the inventory on a quarterly basis and forward a copy of the inventory list and quarterly review to either the AHS contract manager of record, Information Risk Management, or the Information & Privacy Department upon request;

(ii) provide written confirmation that any information and or IT resource destroyed has been destroyed in accordance with the AHS *Records Retention* Schedule, *Official Records Destruction* Procedure, and other AHS policies, procedures, and standards;

(iii) upon expiration or termination of a contract, forward the inventory to AHS and return the information and IT resources listed in the inventory; and

(iv) confirm that no copies of AHS information have been made or retained by the contractor.

4.4 Information Transport, Transmission, and Log

a) Contractors shall ensure that all transportation of AHS information or IT resources, or transmission of information complies with applicable AHS policies, procedures, and standards. Contractors shall maintain accurate

logs to record the internal and external movement of AHS information and IT resources.

5. Access Control

5.1 Contractors shall have in place access control mechanisms and procedures to comply with the provisions of the contract or agreement and AHS *Access to Information (Physical, Electronic, Remote)* Policy and other applicable AHS policies, including but not limited to:

a) Storage

(i) Contractors shall ensure that AHS information and IT resources are securely stored or placed in secure locations to prevent unauthorized access, loss, damage, or corruption.

b) Unattended Equipment

(i) Contractors shall ensure that inactive terminals are automatically logged off from AHS information systems after a defined period of inactivity. Logged-in or otherwise unsecured workstations or **mobile wireless devices** containing or accessing AHS information shall not be left unattended by the contractor.

c) Access Security Audit

(i) Contractors shall maintain a log of all successful and unsuccessful requests for physical, environmental, or electronic access to AHS information and IT resources. The log shall be available, upon request, to Information Risk Management for audit purposes.

6. Incident Management

6.1 All **breaches** shall be immediately assessed by contractors for impact and risk, and appropriate action to mitigate harm and risks shall be taken as soon as possible.

6.2 Contractors shall report all information security incidents involving IT resources or physical access to Information Risk Management as soon as possible. Other breaches shall be reported to Information & Privacy Department. Contractors shall cooperate with any AHS investigation conducted by Information Risk Management and/or the Information & Privacy Departments.

6.3 After receiving and reviewing a report of a breach, either Information Risk Management or the Information & Privacy Department shall advise contractors of appropriate remedies. Any remedial action taken by AHS relating to an information security incident or privacy incident shall be in accordance with legal, contractual, and other AHS requirements.

6.4 AHS shall report required health information breaches to the Office of the Information and Privacy Commissioner of Alberta under the *Health Information Act* (HIA) mandatory breach reporting requirements.

7. Mobile Wireless Device, Laptop, and Mobile Storage Device Security

7.1 Contractor-assigned mobile wireless devices, laptops, and **mobile storage devices** that contain or have access to AHS information or IT resources shall be protected in accordance with AHS policies, procedures, and standards. Mobile wireless devices, laptops, and mobile storage devices shall utilize AHS-approved encryption tools.

7.2 To prevent a loss of information or theft of mobile wireless devices, laptops, or mobile storage devices, contractors shall comply with the requirements set out in the applicable AHS policies and procedures.

7.3 Contractors shall also ensure that all mobile wireless devices, laptops, and mobile storage devices containing or having access to AHS information or IT resources have:

a) an automatic log-off mechanism;

b) processes to prevent unauthorized viewing of user-ids or passwords;

c) encryption in accordance with AHS policies, procedures, and standards;

d) appropriate password protection (e.g., log-on, and screen saver passwords); and

e) AHS approved anti-virus software installed and updated.

8. Information Managers

8.1 Contractors acting as information managers on behalf of AHS shall sign an information management agreement with AHS.

8.2 Information managers may store, retrieve, or dispose of AHS information pursuant to the terms of the information manager agreement and in accordance with applicable legislation and AHS policies. Information disclosed to information managers shall be protected in accordance with applicable legislation and AHS policies.

8.3 Information managers shall not collect, use, disclose or destroy records, including health or personal information, for any purpose other than those authorized by the information management agreement and in accordance with applicable legislation and AHS policies.

DEFINITIONS

Access privileges means privileges granted to contractors for the use of AHS information or IT resources to perform contracted responsibilities. Access privileges may be granted for physical, environmental or electronic resources.

AHS people means Alberta Health Services employees, members of the medical and midwifery staffs, Students, Volunteers, and other persons acting on behalf of AHS (including contracted service providers as necessary).

Breach means a failure to observe security or privacy processes, procedures, or policies, whether deliberate or accidental, which results in the information being viewed, or having the potential to be, accessed, used, transmitted, or held by unauthorized persons.

Contractor means any affiliate, third party, non-employee, consultant, or agent or employee to the contractor, outsourcer, service provider, contract provider or business partner engaged by Alberta Health Services to perform services for or on behalf of Alberta Health Services.

Facility designate means the individual or department responsible for ensuring access controls are met at an AHS facility. A facility designate shall be identified in facilities where AHS Protective Services is not employed.

Information security incident means any incident where there is a violation or breach of the security of information or a weakness or malfunction of IT infrastructure that could potentially cause a violation or breach, is identified.

Information technology (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 wireless devices, and mobile storage 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), and other similar devices.

Mobile wireless devices means smartphones, cellular phones, tablet computers (e.g. iPads) excluding laptop computers, wireless data cards (air-cards), mobile data terminals (MDT), two-way radios, and pagers.

Privacy Impact Assessment means a documented process to assist AHS in reviewing the impact new projects might have on individual privacy.

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.

REFERENCES

- Alberta Health Services Governance Documents:
  - *Access to Information (Physical, Electronic, Remote)* Policy (#1105)
  - *Business Continuity Planning for IT Resources* Policy (#1140)
  - *Collection, Access, Use, and Disclosure of Information* Policy (#1112)
  - *Delegation of Authority and Responsibilities for Compliance with FOIP and the HIA* Policy (#1108)
  - *Information Security and Privacy Safeguards* Policy (#1143)
  - *Information Technology Acceptable Use* Policy (#1109)
  - *Mobile Wireless Devices and Services* Policy (#1160)
  - *Monitoring and Auditing of IT Resources* Policy (#1144)
  - *Official Records Destruction* Procedure (#1133-02)
  - *Privacy Impact Assessments* Policy (#1145)
  - *Privacy Protection and Information Access* Policy (#1177)
  - *Records Retention* Schedule (#1133-01)
  - *Transmission of Information by Facsimile and Electronic Mail* Policy (#1113)
- Non-Alberta Health Services Documents:
  - *Freedom of Information and Protection of Privacy Act* (Alberta)
  - *Health Information Act* (Alberta)
  - International Organization for Standardization (ISO) 27001 and 27002

VERSION HISTORY

Date	Action Taken
January 10, 2012	Revised
October 16, 2019	Revised
Click here to enter a date	Optional: Choose an item