Alberta Health Services

POLICY

TITLE
ACCESS TO INFORMATION (PHYSICAL, ELECTRONIC, REMOTE)

SCOPE
Provincial

DOCUMENT #
1105

APPROVAL AUTHORITY
Corporate Services Executive Committee

INITIAL EFFECTIVE DATE
June 24, 2009

SPONSOR
Legal & Privacy / Information Technology

REVISION EFFECTIVE DATE
January 26, 2021

PARENT DOCUMENT TITLE, TYPE, AND NUMBER
Not applicable

SCHEDULED REVIEW DATE
January 26, 2024

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 Policy Services at policy@ahs.ca. The Policy Services website is the official source of current approved policies, procedures, directives, standards, protocols, and guidelines.

OBJECTIVES

- To ensure Alberta Health Services (AHS) employs consistent physical, administrative, and technical access controls to safeguard patients and **AHS people**, and to protect the security of **information technology (IT) resources** and information, including information processing and storage facilities.

- To support the expected InfoCare behaviours of AHS people when handling information and to meet AHS' legal obligations as a public body holding **personal information** and as a custodian of **health information**.

PRINCIPLES

AHS shall employ physical, administrative, and technical access controls at all facilities for areas containing information classified as **restricted**, **confidential**, or **protected** (see the *Information Classification* Policy), information processing and storage, and IT resources. These controls may include, but are not limited to: surveillance video, alarms, card and key controlled entry doors, access codes, staff identification badges, staffed reception desks, and technical access controls (for example: unique user IDs and passwords).

Capital Management (or designate) is responsible for the management, maintenance, and enforcement of physical access to **AHS facilities**. The prior involvement of Information Technology, Information Risk Management, and/or the Information & Privacy Department is required for decisions to employ new forms of physical, administrative, and technical access controls at AHS facilities. Access levels and privileges shall be restricted to the minimum required to fulfill an individual's roles and responsibilities with AHS. AHS reserves the right to audit and **log** access to information and access controls.

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. Responsibility for Physical Access to AHS Facilities

1.1 Capital Management (or designate) shall:

a) manage AHS facility physical access control and security;

b) establish designated contacts for physical access control, and authorize all access requests prior to issuing access cards, identification badges, keys, access codes, or other physical access control measures; and

c) review AHS facility access rights for **users** regularly.

1.2 Information Risk Management, Capital Management, or the Information & Privacy Department shall periodically, and as appropriate, conduct a physical security assessment of AHS facilities and equipment. The assessment shall be used to identify the security perimeter and applicable security measures to comply with AHS policies, procedures, and standards.

1.3 AHS people shall take reasonable precautions to ensure IT resources are placed in **secure areas** that minimize potential risks from unauthorized access, security threats, and environmental hazards.

2. Physical Access Controls

2.1 Information processing and storage facilities shall be located in secure areas, and protected by a defined security perimeter, security barriers, entry controls, and access controls to protect against unauthorized access, damage, theft, and interference.

2.2 Information Risk Management, in conjunction with Capital Management, or the Information & Privacy Department, shall conduct physical security assessments of AHS facilities, including offices, rooms, and IT resources. The assessments shall identify the perimeter for the secure area and apply the measures necessary for complying with AHS policies, procedures, and standards.

2.3 Individuals aware of a potential or actual threat or **breach** to the integrity of a physical access control shall report the potential or actual threat or breach to Capital Management immediately.

2.4 Capital Management shall complete an incident report about a potential or actual threat or breach to a physical access control and submit such incident report to Information Risk Management or the Information & Privacy Department as

appropriate. Information & Privacy shall report required health information breaches to the Office of the Information and Privacy Commissioner of Alberta in accordance with relevant legislation (as applicable).

2.5 The contact information for Capital Management shall be posted in an area easily visible to all persons entering AHS facilities and communicated to AHS people at all AHS facilities.

2.6 Individuals issued with AHS identification badges shall ensure the badges are clearly visible at all times while the individuals are in AHS facilities.

2.7 Access cards, keys, or identification badges shall not be transferred, loaned, destroyed, duplicated, or marked in any manner by any individual other than Capital Management. The loss or theft of any access card, key, or identification badge shall be reported immediately to Capital Management. Access codes shall be protected and not shared or communicated with anyone who has not been granted access to a secure area.

2.8 Secure areas are restricted to authorized personnel. When applicable, unauthorized personnel may be permitted to visit secure areas when escorted by authorized personnel. Recording equipment (e.g., **mobile wireless devices** and cameras) shall be restricted as required in secure areas.

3. Electronic Access

3.1 Access to AHS information shall only be granted if such access is necessary to fulfill authorized AHS duties and responsibilities. Access shall be to the minimum information necessary to perform the duties and responsibilities in accordance with the AHS *Privacy Protection and Information Access* Policy.

3.2 Information Technology shall create a user access profile based on each user's role with AHS. A record of all users with access privileges to IT resources shall be maintained in accordance with AHS policies, procedures, and standards.

a) IT shall review user access rights, either as part of a regular security review or more frequently (as required), and may revoke or modify privileges when necessary.

b) Information Risk Management shall ensure a formal user management process is in place, including user registration and password management process (see Appendix A), for granting access to information and IT resources.

c) AHS shall grant access to information and IT resources to the level required to perform specified role-related responsibilities.

d) Information Technology shall assign all users a personal and unique user ID. System and application owners shall ensure users with access privileges review and sign the required user agreements to indicate the user understands the conditions of access and agrees to maintain the

confidentiality of system login information. Information Risk Management shall review unusual access activities. Any formal investigations shall be in accordance with AHS' established investigations processes.

3.3 Users shall be responsible for all actions performed under their user ID login. Users shall take the necessary security precautions (e.g., protecting access to workstations) to prevent any user ID misuse.

3.4 Users shall not share or transfer passwords and user IDs to any other person. Users shall be individually responsible for updating and safeguarding their passwords and user IDs, in accordance with AHS policies, procedures, and standards.

3.5 Information Technology shall control and limit access to authorized users for applications, databases, internal and external networks, and 'shared-file' drives. Information Risk Management shall ensure that high-risk IT resources are subject to increased security precautions and measures.

3.6 Any knowledge or suspicion of a threat to the integrity of a password, or where any electronic access control is or may have been compromised, shall be immediately reported to Information Risk Management.

3.7 Any IT resource located in a non-AHS facility or location containing AHS-owned information shall be protected from unauthorized access and environmental hazards in accordance with AHS policies, procedures, and standards.

4. Management of Electronic Access

4.1 Electronic access to IT resources shall require specific login processes, where minimal information is displayed about the system. Information access and dissemination shall be in accordance with the classification system contained in AHS policies, procedures, and standards.

4.2 Special access privileges granted to authorized persons (e.g., system administrators) shall be restricted and controlled. Approval of the specific access privileges granted to an individual based on role shall be required from the Chief Information Officer (or designate).

4.3 Mobile wireless devices, laptops, and **mobile storage devices**, including those used by **contractors**, shall be password controlled and encrypted in accordance with AHS policies, procedures, and standards.

4.4 IT resources used for user access and input, such as workstations, terminals, and other devices, shall automatically log off after a period of inactivity to prevent unauthorized access. IT resources used for user access and input in high-risk locations shall automatically launch a password-protected screensaver after a period of inactivity to prevent unauthorized access. Users shall not leave these IT resources logged-on or be otherwise unsecured or unattended.

5. Remote Access

5.1 **Remote access** to IT resources, and **business information**, health information, or personal information shall comply with applicable AHS policies. Remote access shall be protected and controlled in accordance with AHS policies, procedures, and standards.

6. Termination or Transfer of Employment, Agreement, Contract, or Appointment

6.1 All physical access privileges shall be revoked immediately upon expiration or termination of an individual's employment, agreement, contract, service, or appointment with AHS. All access cards or keys shall be immediately returned to Capital Management.

6.2 Managers, or designates, shall contact Information Technology and Capital Management for the removal of an individual's access privileges.

6.3 Information Technology shall ensure all electronic access privileges, including disabling electronic mail accounts, are revoked upon termination of an individual's employment, contract, service, or appointment with AHS.

6.4 Upon an individual's site transfer or position change, the new manager (or designate) shall ensure access privileges are adjusted to reflect the new position or site requirements.

7. Contractor Access

7.1 Contractors granted access to AHS information or IT resources shall comply with the provisions of the *Contractor Requirements for Security and Privacy of Information and Information Technology Resources* Policy. AHS people responsible for negotiating, administering, and managing AHS contracts shall ensure that all access provisions are met and included as part of the contract, unless otherwise approved by Information Risk Management and the Information & Privacy Department.

7.2 Contractors shall comply with AHS policies, procedures, and standards in all situations both inside and outside AHS facilities when dealing with AHS information and IT resources.

DEFINITIONS

AHS facility means any facility, property, or ground owned, operated, leased, or funded by AHS.

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.

Business information means general information, which is any recorded information about AHS' business activities such as those related to facilities, infrastructure, and security; policies and programs; budgets, expenses, and contracts; reports and statistics, etc., that are under the custody or control of AHS.

Confidential means the classification applied to information where the unauthorized disclosure could cause moderate risk or harm to any individual, AHS, third-party, or to the privacy of individuals, compromise the organization's ability to respond to disaster, or threaten the secure containment of vital records.

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.

Health information means one or both of the following:

a) diagnostic, treatment, and care information; and
b) registration information (e.g., demographics, residency, health services eligibility, or billing).

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.

Log means an electronic or written record of a network, application, or system's activity, used for information, backup, recovery, or review.

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.

Personal information means recorded information, not governed by the *Health Information Act* (Alberta), of any kind stored in any format that identifies an individual including, but not limited to:

a) address and contact information (including an identifying number or symbol assigned to an individual);
b) race, ethnic origin, gender, or marital status;
c) educational, financial, employment, or criminal history;

d) opinions of others about the person;
e) the image of a person on a photograph; and
f) personal views and opinions of a person (except if these are about another person).

Protected means the classification applied to information where unauthorized disclosure could cause low risk or harm to any individual, AHS, or third party. Protected information is available to AHS people who are authorized to view protected information.

Remote access means the ability to connect to a computer network from outside of the AHS network's firewall.

Restricted means the classification applied to information where unauthorized disclosure could cause serious risk or harm to any individual, AHS, third-party, or to the integrity, image, service delivery, or sustainability of AHS.

Secure area means any area where access is restricted to authorized personnel to protect sensitive AHS assets, including IT resources.

User means any person who accesses or uses an IT resource.

REFERENCES

- Appendix A: *Network Authentication Password*
- Alberta Health Services Governance Documents:
  - *Business Continuity Planning for Information Technology Resources* Policy (#1140)
  - *Change Control for Information Technology Resources* Policy (#1141)
  - *Collection, Access, Use, and Disclosure of Information* Policy (#1112)
  - *Contractor Requirements for Security and Privacy of Information and Information Technology Resources* Policy (#1107)
  - *Information Classification* Policy (#1142)
  - *Information Technology Acceptable Use* Policy (#1109)
  - *Mobile Wireless Devices and Services* Policy (#1160)
  - *Monitoring and Auditing of Information Technology Resources* Policy (#1144)
  - *Official Records Destruction* Procedure (#1133-02)
  - *Privacy Protection and Information Access* Policy (#1177)
  - *Records Retention* Schedule (#1133-01)
- Alberta Health Services Forms:
  - *Confidentiality and User Agreement* Form (#07922)
- Alberta Health Services Resources:
  - Access & Disclosure (Health Information Management): disclosure@ahs.ca
  - Information and Privacy: privacy@ahs.ca
  - Whistleblower Line (Confidential): 1-800-661-9675
- 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*

APPENDIX A

Network Authentication Password

1. Password Criteria

1.1 The following requirements apply to AHS passwords:

a) Minimum password length: eight (8) characters.

b) Minimum password age: one (1) day.

c) Maximum password age: 365 days.

d) Enforce password history (uniqueness): 13 passwords remembered.

e) Reset account lockout counter after: 15 minutes.

f) Account lockout duration: 15 minutes.

g) Account lockout threshold: 10 attempts.

h) Password must meet complexity requirements (see Section 2 below): enabled.

i) Store passwords using reversible encryption for all users in the domain: disabled.

2. Password Complexity Requirements

2.1 As the password complexity setting is enabled, user's passwords shall meet the following requirements to access AHS IT resources:

a) The password is at least eight (8) characters long.

b) The password contains characters from at least three (3) of the following five (5) categories:

(i) English uppercase characters (A - Z).

(ii) English lowercase characters (a - z).

(iii) Base 10 digits (0 - 9).

(iv) Non-alphanumeric characters (e.g., !, $, #, or %).

(v) Unicode characters (provide a unique number for every character).

c) The password does not contain three or more characters from the user's account name.

d) The password cannot be a word contained within any dictionary (words in all languages are vulnerable).

3. Exceptions

3.1 If there are system limitations, or other reasons for exceptions, service owners shall ensure that there are adequate password controls in place. Deviations to this Standard shall follow the approved Information Technology exception process, including documentation and authorization from the Chief Information Security Officer, or designate.