Alberta Health Services

POLICY

TITLE
MONITORING AND AUDITING OF INFORMATION TECHNOLOGY RESOURCES

SCOPE
Provincial

DOCUMENT #
1144

APPROVAL AUTHORITY
Corporate Services Executive Committee

INITIAL EFFECTIVE DATE
January 10, 2012

SPONSOR
Information Technology / Legal & Privacy

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 set out requirements for monitoring access to and usage of Alberta Health Services' (AHS) **information technology (IT) resources** and for compliance with applicable AHS policies, procedures, and standards.
- To protect IT resources from unauthorized modification, access, or destruction.
- 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 implement controls to protect logging facilities and **log** files from unauthorized modification, access, or destruction to help AHS protect and maintain the security of IT resources and information in its custody and control.

Periodic independent reviews or audits shall be conducted to confirm that appropriate controls have been implemented and to determine compliance with and measure the effectiveness of AHS' policies, procedures, and standards.

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. Monitoring

1.1 Information Technology and **repository owners** shall ensure that the use of IT resources is monitored to detect authorized and unauthorized accesses, system alerts, and failures. Information Technology and repository owners shall identify the activities to be reported as part of an exception reporting process.

1.2 Monitoring of access to information repositories shall be conducted in compliance with the *Information Classification* Policy and other applicable AHS policies, procedures, and standards.

1.3 AHS' monitoring processes shall be tested through established assurance program cycles annually or at a period determined by a relevant risk assessment to ensure appropriate events are being detected.

2. Audit Logging

2.1 Information Technology, in consultation with repository owners and service owners, shall ensure that audit logs record **user** and system activities, exceptions and information security, and operational events including information about activity on networks, applications, and systems. Audit logs shall be restricted to users with privileged access and be protected accordingly. The user's unique ID shall be included in the audit log.

2.2 Information Technology, repository owners, and service owners shall determine the degree of detail to be logged based on auditing requirements specified in the *Health Information Act* (Alberta) or the Privacy Impact Assessment for the repository, an assessment of the classification of information assets, the criticality of the system, and the resources required to review and analyze the audit logs.

2.3 Audit logs shall be retained in accordance with the AHS *Records Retention* Schedule. Destruction, deletion, purging, overwriting, or alteration of audit logs shall not take place where there is knowledge of, or notification of a **legal hold** or a privacy investigation (see the *Official Records Destruction* Procedure and *Legal Hold* Procedure).

2.4 Repository owners or service owners shall not modify, erase, or deactivate logs of their own activities.

2.5 Logging, while important, shall not take precedence over system performance. In some cases, logging may be limited if it has a significant impact on system performance.

3. Review of Monitoring Activities

3.1 Repository owners shall establish and document processes for reviewing audit logs based on an assessment of the classification of information assets, the

criticality of the system, and the resources required for review. Audit log reviews should, at a minimum:

a) prioritize reviews of high value and highly sensitive information assets;

b) be based on a documented risk assessment;

c) utilize automated tools to identify exceptions (e.g., failed access attempts, unusual activity); and

d) facilitate ongoing analysis and review.

3.2 Access to user IDs and information contained in audit logs to be reviewed shall be as defined in the relevant Privacy Impact Assessment and may include the repository owner, the Information & Privacy Department, and Information Technology.

4. Privileged User Logs

4.1 Information Technology or Information & Privacy, as appropriate, and repository owners shall ensure that the activities of users with privileged access are reviewed regularly and at random by the repository owner (or designate). The frequency of the reviews shall be determined by the classification of information or the criticality of IT resources. Records of verified logs shall be retained in accordance with the *Records Retention* Schedule and applicable policies and procedures.

5. Reporting and Logging Faults

5.1 Information Technology and repository owners shall implement processes for monitoring, reporting, and logging system faults reported by users and automated detection systems. Fault logging requirements should be determined through a risk assessment.

5.2 Information Technology shall review fault logs to ensure that faults have been resolved and regularly report fault incidents and resolution actions to repository owners.

5.3 Where monitoring or auditing processes identify a potential privacy breach, the determination shall be reported to the Information & Privacy Department by the repository owner for follow up as a **breach** investigation (see the *Information Security and Privacy Safeguards* Policy).

DEFINITIONS

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.

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.

Legal hold means a hold placed on the scheduled destruction of records due to foreseeable or pending litigation, governmental investigation, audit, or special organizational requirements as initiated in accordance with the *Legal Hold* Procedure.

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

Repository owner means the individual(s) responsible for defining the processes and controls for the assessment, storage, security, privacy, and disposition of the information in a repository.

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

REFERENCES

- Alberta Health Services Governance Documents:
  - *Access to Information (Physical, Electronic, Remote)* Policy (#1105)
  - *Information Classification* Policy (#1142)
  - *Information Security and Privacy Safeguards* Policy (#1143)
  - *Information Technology Acceptable Use* Policy (#1109)
  - *Legal Hold* Procedure (#1133-04)
  - *Official Records Destruction* Procedure (#1133-02)
  - *Privacy Impact Assessments* Policy (#1145)
  - *Privacy Protection and Information Access* Policy (#1177)
  - *Records Management* Policy (#1133)
  - *Records Retention* Schedule (#1133-01)
- Alberta Health Services Forms:
  - *Confidentiality and User Agreement* Form (#07922)
  - *Privacy Breach Notification* Form (#09579)
- Alberta Health Services Resources:
  - Information and Privacy: privacy@ahs.ca
- Non-Alberta Health Services Documents:
  - *Alberta Electronic Health Record Regulation*
  - *Freedom of Information and Protection of Privacy Act* (Alberta)
  - *Health Information Act* (Alberta)