IMT Standards IMT Standards Oversight Committee Government of Alberta	Effective Date: 2018-10-31 Scheduled Review: 2019-10-01 Last Reviewed: 2018-10-01
	Type: Technical
Standard number - A000089	
Audit Logging Standard	
Category: Security **Keywords: Audit Logging, Security**	

Description of Standard

This standard describes the minimum Audit Log requirements to generate appropriate audit logs, support required audit logging, and log management functions for the Government of Alberta (GoA). This standard applies to all GoA information systems that handle protected information, accept network connections, and make access control decisions.

This Standard supports Information Security Management Directive (ISMD) section 5.24.

An Audit Log is a chronological record of information system activities that is generated by many sources. Sources can include;

- security software such as antivirus software, firewalls, and intrusion detection and prevention systems
- operating systems on servers and workstations
- networking equipment
- applications

Audit logging can provide a means to help accomplish several security related objectives, including individual accountability, reconstruction of events on an information system, intrusion detection, and problem analysis.

Business requirements and the data and information security classification of the information will determine the level of logging that is required.

Standard Specification

These controls are to be performed for audit logs and can apply to either operating system or application audit logs.

1. **Activities to be logged.** Activities to be logged must be determined by the Information Controller after consultation with the Information Custodian. The

audit log shall contain what needs to be monitored and measured, including information security processes and controls.

2. **Elements of the log.** Each log entry must include sufficient information for intended subsequent monitoring and analysis.

   The **minimum** required log elements include:
   - User IDs;
   - Date and time stamp;
   - Description of the activity performed;
   - Reason for logging event (e.g., successful and unsuccessful logon, system and other resource access attempts);
   - Other information that may help to recreate a sequence of event to provide information for investigation purposes;

   Additional Audit log element requirements are determined by the Information Controller.

3. **Log aggregation.** Audit logs must be centrally managed for efficient analysis and reporting. Audit logs may be managed by an application owner, an audit logging tool such as a SIEM, or a supplier.

4. **Log formatting.** Audit logs must be available in a human readable format. The source must support the log data format to ensure the integrity of the logs with the centralized storage and archival system, and support enterprise-level analysis and reporting.

5. **Clock synchronization.** Timestamps in logs must be accurate and synchronized to the single Government of Alberta accepted time source.

6. **Protection of log information.** Logging facilities and the log information must be protected against tampering and unauthorized access. The log protection requirements must be determined by the Information Custodian.

7. **Audit log review.** Audit logs must be reviewed for all auditable security events and unusual activity. The business and security requirements must be developed by the business area. The business area determines the frequency for reviewing audit logs for specific systems and applications based on their criticality and risk profile.

8. **Log storage and disposal.** Audit logs must be stored in a manner that ensures their integrity. Log storage, retention and disposal requirements must be in compliance with the Government of Alberta applicable laws, regulations, and records management requirements.

Where to Apply This Standard

This standard applies to the all GoA departments, boards, agencies and commissions.

Authority and Exceptions

Internal Use Only

Supporting Documentation

1. Information Security Management Directives (ISMD)
2. GoA Data and Information Security Classification standard

Owner

Service Alberta, Office of the Corporate CIO, Corporate Information Security Office (CISO)

Contact

GoA IMT Standards at imt.standards@gov.ab.ca

Additional Information

Audience	Government of Alberta Information and Communications Technology (ICT) environment
Source	Service Alberta, Office of the Corporate CIO, Corporate Information Security Office (CISO)
Sensitivity	Public
Proposed Date	2018-10-01
Proposed By	Corporate Information Security Office Service Alberta ciso@gov.ab.ca

Appendix A

Types of Standards	Description
Technical Standard	These are detailed, unique standards that have developed in response to government IMT policies. Technical standards are intended to be replicable, transferable, and adaptable across ministries and other government agencies. Examples of these could include address data standards or specifications for a single identifier for transacting with government electronically.
Product Standard	An IMT product or specific technology oriented standard that facilitates the task of planning for enhancements and acquisitions within the government's broad information systems environment. As a definitive list of the numerous technologies either employed or under evaluation by Workplace Technology Services, product standards are critical in establishing conformity, interoperability and interchange-ability. Examples of these could include a government-wide standard for document, record management and database, and the list of core products for government workstations.
Process Standard	An established, mandatory business practice that supports IMT projects and existing systems to improve the outcome, diminish risks, and increase reliability. Examples could include business continuity planning processes, threat risk assessment processes, etc.
Reference Standard	An IMT industry standard (either a national or international formal or de facto standard) that has been adopted for use by the Province of Alberta. A Reference Standard may be adopted either as stand-alone or as a precursor to a customized standard or policy document. Examples could include the 1024 bit RSA standard for public key encryption.