		Effective:	7/1/2017
		Last Review:	7/1/2017
Title:	Security Monitoring and Logging	Next Review:	Annually
Number:	ISP-164		
Version:	1.0	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure that State of Alaska (SOA) information systems are monitored to ensure compliance with SOA statutes, Federal regulations, administrative orders, policy, procedures and directives and to provide a record of activity, in the event of a security incident.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- System logging;
- Protection of logging and auditing information;
- System monitoring; and
- Configuring network time protocol (NTP).

5.1. System Logging

5.1.1 Logging

Business Owners must ensure that audit logs recording user activity and information security events are produced by information systems including but not limited to servers, workstations, network devices, and applications. Active audit logs must be retained on a system for not less than 90 days and must be archived for not less than 275 days for a total of 365 days of log retention.

SOA Internal

Business Owners must ensure all Departments' information systems, telecommunications systems and services are directed to a specified State Security Office (SSO) controlled and managed device for the purposes of logging and compliance monitoring.

5.1.2 Minimum Requirement for Event Logging

Business Owners must ensure event logs capture events within a server and application to detect violations and flaws, and assist in reconstruction of user activities for forensic analysis. For each server and application, personnel must log for a minimum of the following:

- User account management activity;
  - addition and deletion of user accounts
  - changes in security attributes (access-levels, logon interval, terminal logon restrictions, connection interface)
  - user account suspensions and reactivations
  - administrative password resets
- Access control related events;
  - successful and failed logon/log-off events
  - account lockout events (invalid password, inactive session, access from un-allowed interfaces, logon attempts out of valid intervals, maximum concurrent session limit violations)
  - password changes
- Changes to application configuration settings must be tracked;
  - change to critical functional settings (e.g. financial interest rates, services charges, grace periods)
  - system parameters (e.g. maximum number of concurrent connections per user, password length)
- Access attempts to applications and underlying system resources;
  - changes to cryptographic keys
  - start-ups/stops of application processes
  - abnormal application exits
  - failed databases connection attempts
  - attempts to modify critical registry keys
  - logon/log-off for maintenance
  - failed integrity checks for application data, executables and audit log.

5.1.3 Log Details Required for Adequate Logging.

Business Owners must ensure logs capture adequate level of detail required for analysis, while balancing the need to not adversely affect performance. The following shall be recorded for each event:

- A unique event ID and type;
- Time stamp of the event
- Error message;
- Success or failure of event;
- IP address for the client;
- User ID triggering the event;
- Resources accessed;
- Application interface used by user; and
- Co-relation with audit trail entries.

SOA Internal

5.1.4 Safe Practices in Logging

Business Owners must ensure Departments apply and follow safe practices in logging. At a minimum, the following practices must be implemented:

- Design the application to save the logs to a different system. Once a system is compromised, the logs will be untrustworthy;
- Secure the system where the logs are stored;
- Limit access to logs on a need-to-know basis;
- Do not log the authentication credentials (e.g. password, PIN or encryption keys) in the log;
- Applications shall alert administrators when a logging system malfunctions or is shut down; and
- The security logs must be archived periodically in accordance with State Archiving requirements.

5.1.5 Administrator and Operator Logs

Business Owners must implement controls to monitor and record the use of system and operator accounts and the actions taken by personnel with system administrator or operator privileges.

5.2. Protection of Log and Audit Information

5.2.1 Protection of Log Data

Business Owners must restrict access to audit logs to only those personnel with a requirement to access the logs, and must ensure that such log data is protected against unauthorized access or modification. Business Owners must establish a process to record access to audit logs.

5.3. System Monitoring

5.3.1 Implementation of Monitoring

Business Owners must implement controls to monitor the use of information systems and information processing facilities. Business Owners must review the results of monitoring activities on a regular basis.

Critical (Life Safety) and sensitive systems or servers must be incorporated into SOA Security Operation Center Services (SOC) monitoring at the department's own expense.

5.4. Configure Network Time Protocol (NTP) - Date and Time Synchronization

5.4.1 Time Synchronization with Date and Time Correlation

All system, services, or networks must reflect the Alaska Time Zone as defined in SOA policy ISP-173 Network Security, § 5.5.6.

SOA Internal