STATE OF ALABAMA

Information Technology Standard

STANDARD 677S1-01: LOG MANAGEMENT

Logs contain information related to many different types of events occurring within systems, networks and applications. Logs serve functions such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating security events. Logs containing records related to computer security may include audit logs that track user authentication attempts and security device logs that record possible attacks. These requirements address security-related logs and log entries.

OBJECTIVE:

Establish the requirements for computer and network resource log management for the State of Alabama computing environment. The goals of log management are:

- Proactive maintenance of information system resources

- Awareness of "normal" vs. "abnormal" network traffic or system performance

- Support after-the-fact investigations of security incidents

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

Organizations responsible for the management and administration of State of Alabama information systems shall define, as part of the System Security Plan, log management procedures that address log generation, transmission, storage, analysis, and disposal.

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-92: Computer Security Log Management, and Special Publication 800-53: Recommended Security Controls for Federal Information Systems, and other best practices, the State of Alabama log management requirements are as follows:

LOG GENERATION

It is not always practical or necessary to log everything; therefore, organizations (system owners and data owners) shall conduct a risk assessment to determine the hosts, host components (e.g., OS, service, application), and events that need to be logged.

Events:

Specify which information system components carry out logging activities. Logging activity can affect information system performance; therefore, decide (based upon a risk assessment) which events require logging on a continuous basis and which events require logging in response to specific situations.

Consider logging the following events:

- Start up and shut down of audit functions

- Successful and unsuccessful logons and logoffs

- Successful and unsuccessful attempts to access security relevant files and utilities, including user authentication information

- Log information on read, modify, or destroy operations

- Configuration changes made during auditing operations

- Unsuccessful usage of user identification or authentication mechanisms

- Changes to the time

- Activities that modify, bypass, or negate system security controls

- Use of privileged accounts

- Administrator logons, changes to the administrator group, and account lockouts

- Actions following log storage failure or exceeding threshold levels

- Unsuccessful security attribute revocations

- Modifications to user groups within a role

- Key recovery requests and associated responses

- Access denials resulting from excessive numbers of logon attempts

- Blocking or blacklisting of user ID, terminal, or access port

- Detected replay attacks

- Rejections of new sessions based on limits to number of concurrent sessions

- Use of compilers

- System software installations

Hosts:

The table below lists the minimum required events to log by host type.

Table 1: Logging Hosts and Event Types

Hosts	Event Category	Event
Domain Controllers, Member Servers	System Event	Success, Failure
Domain Controllers	Policy Change Event	Success
Domain Controllers, Member Servers	Account Management Event	Success
Domain Controllers, Member Servers	Logon Event	Success
Domain Controllers	Account Logon Event	Success
SYSLOG Devices	Codes 0 through 6 (Code 7 optional)	All
Mainframe/RACF	All	Failure, Selected Successes

Frequency:

Log data from servers, network components (switches, routers, etc.) and other critical devices/services shall be collected near-real-time.

Log data from workstations can be collected in batches by polling every 5 minutes (i.e. Agent less) or near-real-time using an Agent, as appropriate.

Log Content:

The information system shall log sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Minimally, log contents shall include:

- Date and time of the event (Time stamps of audit records shall be generated using internal system clocks that are synchronized system wide)
- Component of the information system (e.g., software component, hardware component) where the event occurred
- Type of event
- Subject identity
- Outcome (success or failure) of the event

If the information system provides the capability, include additional, more detailed information in the logs for auditable events including source IP, destination IP, protocol used, and the action taken.

Log data shall be collected in its original form whenever practical but may also be collected in a normalized form (e.g., comma-separated variable (.csv) format) if the normalization takes place at the time of collection and the integrity of the normalized log data is assured.

State approved data encryption and checksums, or a similar process, shall be used to protect the integrity of individual blocks ("time slices") of collected and archived log data.

LOG TRANSMISSION

Identified Log data shall be collected to a centralized, hardened system with restricted physical and remote access that provides both rapid access to current information for network administration and management support as well as a long-term archive of data held in a compressed and secure format for forensic analysis.

LOG STORAGE AND DISPOSAL

Log Retention:

Retain logs for six months to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Ensure that the audit logs for any remote access server authentication mechanism are maintained for no less than a period of 30 days on-line, and one year off-line.

Log preservation means keeping log data that would normally be discarded because it contains activity of particular interest.

Logs pertaining to cyber security incidents shall be preserved in accordance with incident handling procedures.

Log Storage Capacity:

Allocate sufficient log storage capacity and configure logging to prevent such capacity from being exceeded.

Audit Processing:

In the event of an audit failure or log storage capacity being reached, the information system shall alert appropriate organizational officials and take the appropriate action to prevent information system shutdown.

Archived data shall be protected against loss by the same backup process that protects other State data.

Log data that is older than the defined data retention limit for archived data may be deleted from the log collection system, but shall still be available for analysis via the network backup system.

Log Protection:

Utilize strict access control. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

Log data shall always be considered sensitive (unless sanitized for public disclosure).

If logs contain personally identifiable information (PII), the organization shall ensure that the privacy of the log information is protected in accordance with applicable State standards for Sensitive data or PII. Personnel responsible for privacy rule compliance for an organization should be consulted as part of log management planning.

Unauthorized access, or attempted unauthorized access, to logs may be an indication of an attack and shall be treated as a cyber security incident.

LOG ANALYSIS

Make a record of every time logs are reviewed and retain those records. Logs can indicate control, thereby preventing claims of negligence and offering evidence to resolve disputes, therefore, in the legal eye, the records of log review are at least as important as the logs themselves.

Essential items to look for while reviewing logs:

- Attempts to gain access through existing accounts
- Failed file or resource access attempts
- Unauthorized changes to users, groups and services
- Suspicious or unauthorized network traffic patterns
- Recognize which systems are most vulnerable to attack

Access to archived log data shall be restricted to members of IT staff and others as determined by department management.

Auditors may use log data when performing audits.

Cyber Security Incident Response Teams will use the log data when necessary to handle security incidents.

The inadvertent disclosure of sensitive information recorded in logs, such as personally identifiable information (PII), shall be reported to the organization ISO and handled as a cyber security incident.

Log Reduction and Report Generation:

Log reduction, review, and reporting tools shall support after-the-fact investigations of security incidents without altering original audit records.

Activity Review Procedures:

Organizations shall develop and deploy Information System Activity Review Procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Procedures shall address:

- Who is responsible for the overall process and results
- How often reviews will take place
- How often review will results be analyzed
- Organization's sanction policy for employee violations
- Where audit information will reside (e.g., separate server)

- Types of audit trail data and monitoring procedures that will be needed to derive exception reports
- How exception reports or logs will be reviewed
- Where monitoring reports will be filed and maintained
- Mechanisms implemented to assess the effectiveness of the review process (metrics)
- The plan to revise the review process when needed

Monitoring, Analysis, and Reporting:

Regularly review/analyze logs for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

When practical, employ automated mechanisms to integrate monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Daily Review:

- "Error" and "Warning" events from Windows Server logs
- All logged events from domain controller security logs
- All logged events from firewall and Web Server security logs
- SYSLOG devices (e.g., UNIX, Nortel): errors of severity code 0 thru 4 (see Table 2: SYSLOG Severity Codes, below)

Table 2: SYSLOG Severity Codes [RFC 3164]

Code	Key Word	Severity/Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	Informational messages
7	Debug	Debug-level messages

Take immediate action on events identified as critical to network performance/function and events that may reflect unauthorized or illegal activity. Events not requiring immediate action shall be scheduled for review within the week.

Weekly Review:

- All access audit logs
- "Error" and "Warning" events from Windows Workstation logs
- All logged events from File Server and Application Server (other than Firewall and Web Server) Security Logs
- Application Logs (e.g. Exchange, IIS, ISA Server, FTP Server, etc.)
- SYSLOG Devices: errors of severity 5 and 6 (see Table 2: SYSLOG Severity Codes, above)

Patterns indicating unauthorized, suspicious, or illegal behavior will be brought to the attention of appropriate management and an action plan determined. Immediate action shall be taken on events identified as critical to network/system performance/function or events that may reflect unauthorized or illegal activity. Events not requiring immediate action will be identified and scheduled for review.

SUPPORTING DOCUMENTS:

- Information Technology Policy 677: Log Management

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
670-06S1	12/12/2006	Original document
677S1-00	09/01/2011	Replaces Standard 670-06S1 (number and format change only)
677S1-01	01/18/2012	Made logging of SYSLOG severity code 7 (debug) messages optional