OIT Standards for System Logging

Table of Contents

1.0 Purpose....1
2.0 Scope....1
3.0 Exceptions....1
4.0 Requirements....1
4.1 System Logging and Monitoring....1
4.2 Protection of Log Information....1
4.3 Retention and Disposal of Log Information....1
5.0 Time Synchronization....2
6.0 Log Requirements Related to Sensitive Information....2
Appendix A Suggested Items for Logging....2
A.1 Types of Events/Activities....2
A.2 Types of Information to Log about Events....3

1.0 Purpose

The purpose of these standards is to ensure that adequate system and application log file information is recorded, monitored and maintained for the ongoing support and maintenance of systems and applications as well as to comply with any applicable contractual or regulatory requirements related to data security.

2.0 Scope

These standards apply to security systems, network devices and computer servers administered by OIT.

3.0 Exceptions

Exceptions to these standards will be documented in accordance with the UA Security Policy Exception Reporting Process (Under Development).

4.0 Requirements

4.1 System Logging and Monitoring

- The types of activities and events to be logged will be determined by the system and network administrators responsible for the maintenance of the systems and will be based on a variety of factors that include, but are not limited to, the type of system and/or classification level of the data that is stored, processed or transmitted. Appendix A outlines suggested items for logging.
- System logs will be monitored on a regular basis. Log monitoring software should be used where possible.

4.2 Protection of Log Information

- Access to system logs will be restricted to only those personnel with a work requirement to access them.
- Logs should be saved to a central log server or media that is difficult to alter to protect them in the event of a system compromise.
- Log files that contain sensitive information, as defined in the UA Minimum Data Security Standard (Under Development), should be secured in accordance with the controls established for that data.

4.3 Retention and Disposal of Log Information

- Log files will be retained on line for 90 days. Backups of log files will be maintained in accordance with the Standardized Backup Procedures for UAF and Remote Campus

4.3 (continued) Retention and Disposal of Log Information

Locations.

- Log files that contain sensitive information should be disposed of in a secure manner when no longer required.

5.0 Time Synchronization

The date and time of systems being monitored will be synchronized to ntp.alaska.edu.

6.0 Log Requirements Related to Sensitive Information

Additional logging and monitoring requirements may apply for systems that store, process or transmit sensitive data and will be based on applicable contractual or regulatory requirements that pertain to the data. These additional requirements may include:

- Log integrity checking
- Log alerting
- Auditing for specific types of security events/activities
- Other log retention requirements

Appendix A Suggested Items for Logging

A.1 Types of Events/Activities

User Account Activity

- Successful and failed logins, including the location from which the logins or attempts originated
- Successful and unsuccessful file access
- Password changes

User Account Management

- User account management activity including the addition and deletion of user accounts
- Account lockout events such as invalid password, inactive session, login attempts outside of valid intervals, maximum concurrent session limit violations

Privileged Accounts

- Use of administrative privileges
- Administrative password resets

Application and Database Logs

- Application logs for network services such as http and ssh
- Changes to application configuration settings
- Startup/stops of application processes
- Abnormal application exits
- Failed database connection attempts

System

- Changes to system parameters such as maximum number of concurrent connections per user, password parameters
- Changes to cryptographic keys
- Attempts to modify critical registry keys
- Failed integrity checks for application data, executables and audit logs
- Changes in security attributes such as access-levels

Appendix A (continued) Suggested Items for Logging

A.2 Types of Information to Log about Events

- A unique event ID and type
- Time stamp of the event
- Error message
- Success or failure of event
- Resources accessed
- Application interface used by user
- Origination of event (user id, IP address, other)
- Identity or name of affected data, system component or resource