State of Iowa Enterprise Logging Security Standard

May 9, 2016

Purpose

This standard establishes the minimum requirements for collection, storage and review of log information.

Overview

Logging is needed to identify and respond to unauthorized activities on agency systems.

Scope

This standard applies to all participating agencies as defined by Iowa Code Chapter 8B.1(7). Non-participating agencies are encouraged to follow this and other enterprise standards.

Definitions

Selected terms used in the Enterprise Logging Security Standard are defined below:

- **Event**: Something that occurs within a system or network.

Enterprise Logging Standard

1. **Logging**: All servers, network devices, and applications shall be capable of and configured to:
    a. Produce audit logs, and
    b. Off load audit log data to a log aggregation server.

2. **Events**: The following events (successful and failed) shall be captured in audit logs:
    a. Authentication attempts,
    b. Attempts to use a privileged account,
    c. Attempts to change account passwords,
    d. Attempts to modify or destroy a log file, and
    e. Attempts to grant, modify, or revoke access rights.

The following shall be logged for each event:

    f. User/subject identity,
    g. Date and time of the event,

h. Source of access,
i. Duration of access,
j. Actions executed, and
k. Action result.

3. **Applications**: Applications, including web services and database services, residing on servers that utilize cached or separate authentication capabilities must also maintain logs of all security, application and event related information. Web applications shall also meet the requirements of Enterprise Web Application Security Standard.

4. **Storage**: The System Administrator will ensure audit storage capacity is allocated in accordance with system configuration such that capacity is not exceeded.

5. **Log Access**: Audit records, audit settings, and audit reports shall be protected from unauthorized access, modification, and deletion.

6. **Alerts**: Where feasible systems shall be configured to provide real-time alerts for the following:
   a. Audit failure.
   b. Escalation of privileges.
   c. Five (5) or more consecutive failed authentication attempts.

7. **Time Stamps**: Systems shall be configured to generate time stamps to include both date and time. The time may be expressed in Coordinated Universal Time (UTC) and utilize Network Time Protocol (NTP) time synchronization.

8. **Retention:** Audit logs shall be retained for a minimum of 45 days. Maximum log retention shall be set to meet agency contractual requirements.

9. **Review**: Audit logs shall be reviewed at least weekly. Alerts shall be reviewed daily.

10. **Providers**: Third party providers shall meet the requirements of this standard.

Updates This document shall be reviewed at least every two years and updated as needed.

Effective Date This standard shall be effective May 9, 2016.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A) and Iowa Code 8B.21(1)(f)(2).

Variance Iowa Administrative Code 11 - 25.11(2) and Iowa Code 8B.21(5) provide for variances\waivers from security standards. Requests for a variance\waiver from any of the requirements of this standard shall be submitted in writing to the Chief Information Security Officer.