8-708. Logging; audit review, monitoring, findings and remediation.

(1) Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. Additionally, these logs must be reviewed by authorized personnel to facilitate investigations of suspicious activity or suspected violations. All reports of findings must be reported to appropriate officials who will prescribe the appropriate and necessary actions. Logs must be reviewed as follows:

(a) Logs of suspicious activity must be reviewed as soon as possible;

(b) Logs of system capacity and log integrity must be reviewed on a weekly basis;

(c) Logs of privilege access account creation or modification must be reviewed on a weekly basis; and

(d) All other logs must be reviewed at least monthly.

(2) When possible, the agency or Office of the CIO will employ automated mechanisms to alert the Office of the CIO, state information security officer, or agency information security officer when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis must not change the underlying log structure. It is acceptable for log analysis tools to extract data for analytical review, if the original audit logs remain unchanged and secured.

(3) All relevant findings discovered because of an audit log review must be listed in the appropriate problem tracking system or the corrective action planning process to ensure prompt resolution or appropriate mitigating controls. All results and findings generated by the audit or review process must be provided to appropriate agency management within one week of completion. This report should be considered CONFIDENTIAL information.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-708.pdf