8-709. Logging; application logging review and monitoring.

All state applications must provide logging for security events. Application logs are invaluable data for identifying security incidents, monitoring policy violations, establishing baselines, providing information about problems and unusual conditions, contributing additional application-specific data for incident investigation which is lacking in other log sources, and helping defend against vulnerability identification and exploitation through attack detection.

Application logging content must be part of the overall system analysis and design activity, and should consider:

(1) Application process startup, shutdown, or restart;

(2) Application process abort, failure, or abnormal end;

(3) Significant input and output validation failures;

(4) Business process monitoring (e.g., activity abandonment, transactions, connections, information requests);

(5) Audit trails (e.g., data addition, modification and deletion, data exports);

(6) Performance monitoring (e.g., data load time, page timeouts);

(7) Compliance monitoring and regulatory, legal, or court ordered actions;

(8) Authentication and authorization successes and failures;

(9) Session management failures;

(10) Use of higher-risk functionality (e.g., addition or deletion of application credentials, changes to privileges, assigning users to tokens, adding or deleting tokens, submission of user-generated content - especially file uploads); and

(11) Suspicious, unacceptable or unexpected behavior.

Application logs must be reviewed at least monthly. Corrective actions to address application deficiencies must be managed through the application development process or the applicable corrective action planning process.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-709.pdf