8-707. Logging; audit log contents.

Audit logs must contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The logs must identify or contain at least the following elements, or enough information in which to infer the following elements with reasonable assurance:

(1) Type of action (e.g., authorize, create, read, update, delete, and accept network connection);

(2) Subsystem performing the action (e.g., process or transaction name, process or transaction identifier);

(3) Identifiers (as many as available) for the subject requesting the action (e.g., user name, computer name, IP address, and MAC address). Note that such identifiers should be standardized to facilitate log correlation;

(4) Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;

(5) Whether the action was allowed or denied by access-control mechanisms;

(6) Description or reason-codes of why the action was denied by the access-control mechanism, if applicable; and

(7) Depending on the nature of the event that is logged, there may be other information necessary to collect.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-707.pdf