8-706. Logging; auditable events.

Security safeguard regulations require logging and reviewing events that are determined to have a moderate or above level of risk. Auditable events may be incorporated into system auto logs and change management documents. The following events should be logged and reviewed on a weekly basis:

(1) Log on and off the system;

(2) Change of password;

(3) All system administrator commands, while logged on as system administrator;

(4) Switching accounts or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS);

(5) Creation or modification of super-user groups;

(6) Subset of security administrator commands, while logged on in the security administrator role;

(7) Subset of system administrator commands, while logged on in the user role;

(8) Clearing of the audit log file;

(9) Startup and shutdown of audit functions;

(10) Use of identification and authentication mechanisms (e.g., user ID and password);

(11) Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);

(12) Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;

(13) Changes made to an application or database by a batch file;

(14) Application-critical record changes;

(15) Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);

(16) All system and data interactions concerning FTI;

(17) Additional platform-specific events, as defined by agency needs or requirements;

(18) Detection of suspicious or malicious activity such as from an intrusion detection or prevention system (IDS/IPS), anti-virus system, or anti-spyware system; and

(19) Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-706.pdf