

8-705. Logging; format, storage, and retention.

The state is required to ensure the availability of audit log information that is subject to federal audit by allocating sufficient audit record storage capacity to meet policy requirements. Office of the CIO and the agency IT teams shall perform annual capacity planning and trend analysis to reduce the likelihood of such capacity being exceeded. The capacity and utilization of log files must be regularly monitored and reported, and action will be taken to keep an approved level of free space available for use. Automated notification of agency or Office of the CIO personnel must occur if the capacity of log files reaches defined threshold levels, or the audit logging system fails for any reason.

The audit logging process is required to provide system alerts to appropriate agency or Office of the CIO personnel in the event of an audit processing failure (e.g., shut down information system, unintended overwriting of the oldest audit records, stop generating audit records). All system logs must be sent to a central log review system that is protected from unauthorized access and is backed up for availability and integrity purposes. All log files subject to federal audit requirements must be retained for seven years.

--

History: Adopted on July 12, 2017.

URL: <http://nitc.nebraska.gov/standards/8-705.pdf>