8-507. System maintenance.

The following are system maintenance standards:

(1) All systems involved in the processing, storage, or access to any CONFIDENTIAL or RESTRICTED information must be maintained per manufacturer specifications. Maintenance personnel must be approved for this activity by the state information security officer and must be briefed on the requirements for protecting sensitive information;

(2) Maintenance activity must be logged to include the date/time of the maintenance, activity performed, the person or organization who performed the maintenance, the name and department of the escort (if applicable), and a detailed list of any equipment removed or replaced during the maintenance. This list should include serial numbers, if applicable;

(3) Prior to removing any equipment from the secured environment to which it is assigned, the equipment must be approved for release and validated by the state information security officer that all non-public information has been encrypted, secured, or permanently deleted from the equipment. When equipment is returned, it must be inspected for unauthorized systems, settings, or services to ensure the integrity of the security systems before reloading data or placing back into the environment;

(4) All tools used for maintenance must be tested. The Office of the CIO must maintain a list of approved maintenance tools that is reviewed and updated at least annually;

(5) Nonlocal or remote maintenance must be approved in advance by the state information security officer or the Office of the CIO, and must also comply with all agency and Office of the CIO requirements for remote access;

(6) All remote maintenance activity must be logged and reviewed;

(7) Maintenance of agency-developed software must follow the state's change management process to ensure changes are authorized, tested and accepted by agency management. All known security patches must be reviewed, evaluated and appropriately prioritized;

(8) Critical patches must be applied within 24 hours of receipt. High risk patches must be applied within 7 days of receipt. All other patches must be appropriately applied in a timely manner as determined by the agency; and

(9) All vendor supplied software deployed and operational must be currently supported by the vendor.

--

History: Adopted on July 12, 2017.

URL: https://nitc.nebraska.gov/standards/8-507.pdf