Technical Panel
of the
Nebraska Information Technology Commission

Technical Standards and Guidelines

Proposal 25

30-Day Comment Period

Notes:

1. The following proposal is under review by the Technical Panel of the Nebraska Information Technology Commission. The proposal modifies the technical standards and guidelines posted at: https://nitc.nebraska.gov/standards/index.html.
2. The panel is seeking comments on this proposal from any interested person or entity.
3. Comments should be sent to: ocio.nitc@nebraska.gov.
4. The comment period for this proposal ends on May 13, 2022.
5. The panel will review this proposal, and any comments received, at a public meeting following the comment period. That meeting is currently scheduled for June 14, 2022. Information about the meeting, including a copy of the agenda, will be posted at: https://nitc.nebraska.gov/technical_panel/meetings/index.html.
6. Contact information: ocio.nitc@nebraska.gov or 402-471-7984.
A PROPOSAL relating to the Information Security Policy; to add a definition; to amend section 8-507; to adopt a new section 8-608 relating to low-code/no-code and containerized development; and to repeal the original sections.

Section 1. Section 1-101 is amended to add the following new subsection, and renumbering the existing subsections accordingly:

“CIS” is an abbreviation for Center for Internet Security, Inc., a nonprofit entity, which develops controls, benchmarks, and best practices for securing IT systems and data. [https://www.cisecurity.org/]

Sec. 2. Section 8-507 is amended to read:

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 state 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;
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;

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;

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;

All remote maintenance activity must be logged and reviewed;

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;

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. Vendor patches must be applied in an order based on organizational risk and must be applied within thirty days of receipt; and

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

Sec. 3. The following new section is adopted:

Low-code/no-code and containerization development.

Low-code/no-code and containerization development platforms are types of visual software development environments that allow enterprise developers to drag and drop application components, connect them together and create mobile or web apps and microservices. These
types of environments allow for the dynamic allocation of resources. While these types of
environments allow for swift and agile development without the necessity to write fully coded
applications, the platforms also present architectural, security and governance challenges. The
following are low-code/no-code and containerization development standards:

(1) All projects involving low-code/no-code in the cloud must be reviewed and approved
by the OCIO Cloud Review Board;

(2) Low-code/no-code projects must maintain compliance with all applicable standards;

and

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

Sec. 4. Original sections 1-101 and 8-507 are repealed.

Sec. 5. This proposal takes effect when approved by the commission.