8-202. Change control management.

To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained.

The change management process may differ between changes to IT infrastructure (which includes all hardware, system software, and network assets) and application software (which includes commercial off the shelf data applications and in-house developed data application software). However, underlying requirements for managing change are the same. All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release and does not unknowingly add security risks to the state's environment. All changes to network perimeter protection devices should be included in the scope of change management.

(1) IT Infrastructure. The following change management standards are required to be followed for all IT infrastructure:

(a) The Office of the CIO requires a change management process with assigned responsibilities to ensure all changes to hardware, system software, and network infrastructure are authorized. This process will include representation from the Office of the CIO, agency, state information security officer, and application development (when application changes impact or are impacted). This process must occur on a periodic basis with sufficient frequency to meet demands for changes to the environment;

(b) All records, meetings, decisions, and rationale of the change control group must be documented and securely stored for audit purposes. The agenda for this meeting is flexible but should generally address a review of at least the following: (1) change summary, justification and timeline; (2) functionality, regression, integrity, and security test plans and results; (3) security review and impact analysis; (4) documentation and baseline updates; and (5) implementation timeline and recovery plans;

(c) The agency is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as CONFIDENTIAL information, and secured appropriately. The baseline documents must be reviewed and updated on an annual basis or after any significant changes to the baseline have been installed; and

(d) All changes to the production infrastructure are required to be made by authorized personnel only, using access credentials assigned to that individual. Actions performed by these user credentials will be logged.

(2) Application Development. The following change management standards are required to be followed for application software systems that create, process, or store CONFIDENTIAL or RESTRICTED data:

(a) Application change management processes must be performed with assigned responsibilities to ensure all changes to application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements;

(b) The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request;

(c) The change management processes will retain a documented history of the change process as it passes through the software development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following: (1) change summary, justification, and timeline; (2) functionality, regression, customer acceptance, and security test plans; (3) security review and impact analysis; (4) documentation and baseline updates; and (5) implementation timeline and recovery plans;

(d) Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must be implemented;

(e) Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place that ensure the confidentiality, integrity, and availability of the data maintained in the production library; and

(f) Application development changes that impact IT infrastructure must be submitted to the infrastructure change management process for review, approval, and implementation coordination.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-202.pdf