8-604. Application development.

The following standards are required to be followed for agency developed application software that create, process, or store CONFIDENTIAL or RESTRICTED data:

(1) The agency must establish an application change management processes with assigned responsibilities to ensure all changes to applicable application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements;

(2) 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;

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

(4) 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;

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

(6) Application development changes that impact agency IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation;

(7) The security requirements of new applications must be established, documented and tested prior to their acceptance and use. The agency information security officer must ensure that acceptance criteria are utilized for new applications and upgrades. Acceptance testing must be performed to ensure security requirements are met prior to the application being migrated to the production environment;

(8) All applications are required to maintain up-to-date documentation that includes an assessment of security threats and impacts, and a detailed description of the data handling with its accurate classification;

(9) Applications that provide user interfaces must have an appropriate warning banner displayed, applicable to the data being accessed (e.g., PHI, FTI, PII);

(10) Application credentials, where possible, should be inherited from the state managed authentication source. If that is not possible, credentials should have the same level of management and approval as other agency access credentials; and

(11) Applications must be configured such that CONFIDENTIAL or RESTRICTED data will be encrypted when transmitted outside the agency internal network.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-604.pdf