8-701. Auditing and compliance; responsibilities; review.

It is the responsibility of the state information security officer to ensure an appropriate level of security oversight is occurring at all potential exposure points of state and agency systems and operations so that the state has reasonable assurance that the overall security posture continuously remains intact. The state information security officer and agency information security officer have the responsibility to ensure the overall security program meets state and federal legal requirements.

The state information security officer will establish and manage an entity-wide oversight and compliance function. This will include, at a minimum, appropriate information security oversight at key points within the technology acquisition process, hardware and software change management process, and the contract management process when changes involve access to or potential exposure of CONFIDENTIAL or RESTRICTED information.

Compliance with this policy is mandatory. Any compromise or suspected compromise of this policy must be reported as soon as reasonably possible to appropriate agency management and the state information security officer.

An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.

The state information security officer may periodically review agency compliance with this policy and the related NIST control framework. Such reviews may include: (1) reviews of the technical and business analyses required to be developed pursuant to this policy; and (2) project documentation, technologies or systems which are the subject of the published policy or standard.

These additional reviews may occur due to significant changes in technical infrastructure, or to validate corrective actions after a security incident. All identified gaps or deficiencies must be documented in an agency security corrective action plan that shall be made available to the state information security officer as necessary. This plan is classified as a RESTRICTED information document, and should contain detailed descriptions of the security deficiencies, recommended remediation or mitigation activity, key milestones and target dates, and responsible parties. This plan should be a regular item for review by senior agency and Office of the CIO management to ensure acceptable progress is being made on mitigating or remediating security gaps.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-701.pdf