8-702. Awareness and training.

(1) The state provides information technology resources to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations subject to state government policies and applicable state and federal laws. It is the responsibility of all staff to protect information resources and ensure that such resources are not misused.

An information security awareness program must be developed, implemented, documented, and maintained that addresses the security education needs of the state. To ensure staff is knowledgeable of security procedures, their role and responsibilities regarding the protection of agency information and the proper use of information processing to minimize security risks, all staff with access to agency information must receive security awareness training, which must be reinforced at least annually. Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities.

(2) New Hire and Refresher Training. All new hires must complete security training, including information about this policy, as part of their orientation. On an annual basis, all staff must complete a security and privacy training session. The state will maintain records of all attendance for new hire and refresher training.

(3) Simulated Phishing. Phishing is a significant threat vector for the state's technology environment. To aid in mitigating this threat and raise awareness of the tactics and techniques used by malicious actors to compromise credentials, simulated phishing campaigns will be conducted at least annually by the Office of the CIO. Anonymized reports may be provided on a per agency basis upon request.

(4) Security Briefings. Management should periodically incorporate information security topics into their meetings with staff. Additionally, the state information security officer may require periodic security briefings to selected audiences when circumstances require, such as responding to a gap in security policy or addressing recurrence of security incidents.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-702.pdf