8-803. Penetration testing.

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to state penetration testing and intrusion testing. Penetration and intrusion testing will be conducted at the request of the agency or data owner(s) to determine if unauthorized access and or changes to an application can be made.

The results of the penetration and intrusion testing will be reviewed in a timely manner by the state information security officer. Any vulnerability detected will be evaluated for risk by the agency and a mitigation plan will be created and forwarded to the state information security officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for penetration and intrusion testing must be coordinated by both entities.

Any penetration or intrusion testing must be performed by individuals who are authorized by the state information security officer and who have requested and received written consent from the Office of the CIO at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or vulnerability scanning must have a process defined, tested and followed to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-803.pdf