8-804. Vulnerability scanning.

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 vulnerability scanning.

All servers will be scanned for vulnerabilities and weaknesses by the Office of the CIO before being installed on the state network. For both internal and external systems, scans will be performed at least monthly or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. Priority setting of vulnerabilities will be based on impact to the state and as referenced in the National Vulnerability Database (http://nvd.nist.gov).

All web-based applications will be scanned for vulnerabilities and weaknesses before being promoted to a production environment or after any major upgrades or changes have occurred. Results of the vulnerability scan will be reviewed in a timely manner by the state information security officer. Any vulnerability detected will be evaluated for risk by the Office of the CIO or agency and a mitigation plan will be created as required 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 vulnerability scanning must be coordinated by both entities.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-804.pdf