8-401. Network documentation.

The State of Nebraska encourages the use of its electronic communications infrastructure in support of its mission. However, this infrastructure must be well-managed and protected to ensure the security of Agency information. Therefore, all network devices that access the state internal network are required to adhere to these standards.

The Office of the CIO and agencies will implement a range of network controls to ensure the confidentiality, integrity, and availability of the data flowing across its trusted, internal network, and ensure the protection of connected services and networks. The Office of the CIO ensures that measures are in place to mitigate security risks created by connecting the state network to a third party network. All direct connections to the state network and direct connections between agencies must be authorized by the Office of the CIO.

Where an agency has outsourced a server or application to an external service provider (such as a web application), the agency must perform or have performed a security review of the outsourced environment to ensure the confidentiality, integrity, and availability of the state's information and application is maintained. For applications hosted by Nebraska.gov, the Nebraska State Records Board will perform the security review on behalf of all agencies.

All publicly accessible devices attached to the state network must be registered and documented in the IT inventory system. Additions or changes to network configurations, including through the use of external service providers, must be reviewed and approved through the Office of the CIO's change management process. Publicly accessible devices must reside in the Office of the CIO's DMZ unless approved by the Office of the CIO for legitimate business purposes.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-401.pdf