8-402. Network transmission security.

The following are network transmission security requirements:

(1) All encryption must be approved by the state information security officer. Any transmissions over unsecured networks (such as the Internet) that contain CONFIDENTIAL or RESTRICTED information must be encrypted using technology that is FIPS 140-2 compliant;

(2) Network scanning and monitoring is prohibited, unless prior approval is obtained from the Office of the CIO. If approved, scanning must be restricted to authorized and registered IP addresses only, and conducted by authorized personnel only;

(3) The Office of the CIO shall ensure that all networks and systems are monitored 24x7 with authorized tools (such as network based intrusion detection and prevention systems) and personnel to detect system anomalies or security events; and

(4) Passwords and SNMP community names may not be sent in clear text over open networks. All devices must use authorized encryption for access authorization to the state network. Access to the DMZ applications is exempt from this requirement.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-402.pdf