8-301. Remote access.

It is the responsibility of all agencies to strictly control remote access from any device that connects from outside of the state network to a desktop, server or network device inside the state network and ensure that employees, contractors, vendors, and any other agent granted remote access privileges to any state network utilize only approved secure remote access tools and procedures.

The following are the requirements for remote access:

(1) Requests for remote access must be reviewed and approved by the agency and the Office of the CIO;

(2) All remote sessions must use access control credentials and an OCIO-approved form of multi-factor authentication;

(3) All remote sessions must utilize OCIO-approved cryptographic mechanisms as defined by NIST 800-140 to protect the confidentiality and integrity of remote access sessions;

(4) All remote sessions over open public networks must use a VPN when connecting to the state network;

(5) All devices connecting to the network must have up-to-date anti-virus protection, active firewalls, and appropriate security patch levels equivalent to those provided for state equipment;

(6) All remote state owned or managed devices must be password protected and full-disk encrypted using OCIO-approved technology;

(7) All remote access sessions must be logged. The Office of the CIO or the agency will perform periodic monitoring of remote access sessions with random inspections of the user security settings and protocols to ensure compliance with this policy;

(8) Remote access logon failures must be logged. Credentials must be disabled after three (3) consecutive failed login attempts;

(9) Remote sessions must be locked after no more than 15 minutes of inactivity until the user re-establishes access with the appropriate credentials and authentication procedures;

(10) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information (e.g., SSA, FTI, PII, PHI) cannot be downloaded or remotely stored; and

(11) Restricted data types cannot be accessed by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations.

--

History: Adopted on July 12, 2017. Amended on November 4, 2021.
URL: https://nitc.nebraska.gov/standards/8-301.pdf