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 standards apply to all staff that connect to the state network through the Internet. This includes all approved work-from-home arrangements requiring access to state systems and agency office locations that use the Internet to access the state network. Each state agency will be responsible for ensuring that remote access to state resources is secured and compliant with this policy.

(1) The following are the general requirements for remote access:

(a) Requests for remote access must be reviewed and approved by the state information security officer and the agency information security officer prior to access being granted;

(b) Staff approved for remote connectivity are required to comply with all policies and standards;

(c) 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;

(d) 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;

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

(f) 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; and

(g) Staff with remote access privileges must ensure that their computer which is remotely connected to the state network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

(2) The following are additional requirements for remote access to data classified as CONFIDENTIAL or RESTRICTED:

(a) Requests for remoted access must indicate if CONFIDENTIAL or RESTICTED data may be accessed;

(b) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information cannot be downloaded or remotely stored;

(c) All state owned or managed devices must be password protected and full-disk encrypted using approved technology. Encryption technology must be provided or approved by the Office of the CIO; and

(d) Remote sessions that store, process, or access CONFIDENTIAL or RESTRICTED information or systems must use access control credentials and an approved form of multi-factor authentication before connecting to the state network. Remote sessions must employ Office of the CIO approved cryptography during the entire session when connected to the state network.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-301.pdf