8-506. Minimum mobile device configuration.

All mobile computing devices accessing the state network or containing state information must be provisioned to meet these security policies and be approved by the Office of the CIO. All devices that will be connected to the state network must be logged with device type and approval date. The following are minimum mobile device configuration standards:

(1) Mobile computing devices must be shut down or locked when not in use. These devices must not be left unattended in a public access area. They must be locked in a secure cabinet or room, or kept on the person. Devices should not be shared;

(2) Mobile computing devices and mobile storage devices must not be left in a vehicle unattended;

(3) Storing CONFIDENTIAL or RESTRICTED information on any mobile device or any removable or portable media (e.g., CDs, thumb drives, DVDs) is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the state information security officer. In those cases, all mobile computing devices or portable media shall be encrypted using technology that is approved by the state information security officer;

(4) Personally owned mobile devices (e.g., smartphones and tablets) may be used for approved state purposes, including email, when configured to access the state information through a managed interface or sandbox only. Devices that are not configured to use the authorized interface are prohibited from accessing any state information, including email;

(5) The device must have security settings that block users from changing mandatory settings;

(6) Strong passwords are required, and passwords must change regularly per state policy regarding passwords;

(7) The device must lock after no more than 5 minutes of inactivity and must require the re-entry of a password or PIN code to unlock;

(8) After 10 unsuccessful password attempts, the device or the state container will be erased. In the event that the device becomes lost or stolen, the Office of the CIO must have the capability to remotely locate, lock, and erase the device;

(9) The device should have all data backed up at the state data center;

(10) Devices need to be cleared of all information from the prior user before being issued to a new user;

(11) The device OS must be up to date and patched. New versions of the OS must be vetted for security posture and supportability;

(12) Devices must be properly disposed of using mechanisms approved by the state information security officer. State data must be cleared and devices properly disposed of or recycled. The disposition process is required to be documented and periodically audited; and

(13) New devices are required to be configured and operate within established security guidelines and help desk support must be established before these devices can be operational. New devices need to be validated before being made available for users to request.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-506.pdf