

8-203. Multi-function devices.

All multi-function devices used to process, store, or transmit data must be approved by the state information security officer or agency information security officer. The device must be configured and managed to adequately protect sensitive information.

Configuration and management of multi-function devices must include minimum necessary access to the processing, storing, or transmitting functions. All unnecessary network protocols and services must be disabled. Access controls must be in place, and administrator privileges must be controlled and monitored. Auditing and logging must be enabled. Access to the internal storage must be physically controlled. The devices must be securely disposed or cleansed when no longer needed. Software and firmware must be updated to the latest version supported by the vendor. All CONFIDENTIAL or RESTRICTED information must be encrypted in transit when moving across a WAN as well as when stored on the internal storage unit of the device. If the device stores information and is not capable of encrypting internal storage, then it must be physically secured or not used for CONFIDENTIAL or RESTRICTED information. Encryption technology must be approved by the state information security officer or agency information security officer.

--

History: Adopted on July 12, 2017.

URL: <http://nitc.nebraska.gov/standards/8-203.pdf>