Technical Panel
of the
Nebraska Information Technology Commission

Technical Standards and Guidelines

Proposal 34

30-Day Comment Period

Notes:

1. The following proposal is under review by the Technical Panel of the Nebraska Information Technology Commission. The proposal modifies the technical standards and guidelines posted at: https://nitc.nebraska.gov/standards/index.html.
2. The panel is seeking comments on this proposal from any interested person or entity.
3. Comments should be sent to: ocio.nitc@nebraska.gov.
4. The comment period for this proposal ends on March 22, 2024.
5. Contact information: ocio.nitc@nebraska.gov or 402-471-7984.

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 34

A PROPOSAL to adopt a new section relating to international travel.

Section 1. The following new section is adopted:

8-213. International travel.

International travel increases cyber risks to the information technology infrastructure of the State of Nebraska. These risks include the use of unsecured public Wi-Fi, device loss, data loss, and cyber espionage. To mitigate these risks, anyone traveling outside the legal jurisdictional boundary of the United States (outside of the United States, its territories, embassies, or military installations) must comply with cybersecurity best practices. The following are requirements when traveling internationally:

(1) If traveling with a state-issued device, you must contact the Office of the CIO at least 72 hours prior to departure. In part, this is to avoid service disruptions and international data charges on mobile devices;

(2) Always maintain positive control over devices. Never leave a device unattended and do not place in checked baggage;

(3) Multi-factor authentication must be used to access state resources;

(4) OCIO-approved VPN must be used to access state resources;

(5) State-issued devices must have full disk encryption enable to prevent unauthorized access to your data in case a device is lost or stolen;

(6) Software and operating systems must be patched and up to date with the latest patches and updates to mitigate known vulnerabilities and limit cyber risk exposure and attack surface;

(7) User passwords should be changed before leaving to ensure they do not expire while traveling. User passwords must be changed after returning to ensure that they are safe in the event that any may have become compromised while traveling;

(8) Only certain state personnel will be able to access OWA or other cloud-based resources when traveling internationally. This means that email on mobile devices may not update automatically;

(9) Based on the level of threat and risk from the region of travel, the state information security officer may restrict access to certain state resources; and

(10) All state-issued devices must be factory reset, or wiped, upon return. The agency may contact the Office of the CIO to obtain temporary loaner equipment to be used while traveling internationally.

Sec. 2. This proposal takes effect when approved by the commission.