NORTH Dakota | Information Technology
Be Legendary.

Created: 07/05/2022
Revised: 08/18/2025
Reviewed: 08/18/2025

International Traveler Guidelines

Overview

International travel creates additional risk when trying to access data and systems. This is especially true for government team members. In addition to physical risks such as theft, loss, and damage of devices, foreign travelers are susceptible to social engineering techniques and a wide range of cyberattacks. Government team members are lucrative targets of nation-state hackers and cyber criminals.

State and personal devices can contain sensitive information, which may be valuable to such actors to sell or to use in intelligence operations. Thus, it is imperative as an team member of the State of North Dakota to exercise due diligence in protecting sensitive data. While travelling abroad, you are responsible for the security of devices and data.

Scope

The guidelines apply to any State team member who must travel to a foreign country with a state-owned device (e.g., work laptop) and/or a personal device with access to state data (e.g., personal cell phone used for work). This guidance is in accordance with the Remote User Access Standard.

Note: The State of North Dakota restricts team members from taking state devices out of the country while travelling for personal reasons unless approved by the team member's agency.

Prior to Departure

Take proactive steps to secure your devices and your personally identifiable information (such as your name, address, date of birth and Social Security Number) before you travel. Leave at home any electronic equipment you don't need during your travel. If you take it, protect it. Be sure to:

- Back up your personal devices
- Consider using a burner device and not taking your primary equipment
- Install encrypted text messaging app (e.g., Signal, etc.) for phones if texting is needed
- Remove sensitive data
- Ensure passwords are complex, and do not use the same password for multiple sites
- Confirm antivirus software is up-to-date
- Have your manager or agency's HR department submit a ServiceNow Generic Service Request, at least two weeks prior to travel, indicating:
    - Your destination
    - Dates of departure and return
    - Hotel name(s) and address(s)

- Which state-owned device(s) you will be taking out of the country (if applicable)
- Which personal devices you will be taking out of the country and will need access to State data (if applicable)

NDIT HR will confirm with agency HR on approval for access. Then, NDIT GRC will notify NDIT Cyber Analysis and Response of your travel plans to ensure that you retain access to your device while travelling. Desktop Support will ensure "Always on VPN" is configured on the state-owned device, hard drive is encrypted, and malware protection is up-to-date (if travelling with a state-owned device).

During Travel

Be vigilant about your surroundings and where and how you use your devices. Make sure to keep your devices secure in public places such as airports, hotels and restaurants. Take care to ensure no one is trying to steal information from you by spying on your device screen while it is in use.

You are especially vulnerable in locations with public Wi-Fi, including:

Internet cafes, coffee shops, bookstores, travel agencies, clinics, libraries, airports and hotels.

- Do not trust public Wi-Fi
- Do not use the same passwords or PIN numbers abroad that you use in the United States
- Never use public Wi-Fi to make online purchases or access bank accounts. Always use a VPN
- Do not use texting to send sensitive information. Consider using an enterprise approved communication application that encrypts communication. Signal is an example of an encrypted communication application.
- Avoid using public equipment – such as phones, computers and fax machines – for sensitive communications
- Keep your device(s) in a locked safe or locked suitcase when leaving your hotel room
- Refrain from logging into social media accounts
- Do not draw excessive attention to yourself. Do your best to blend in and keep a low profile
- Be mindful of what you say and do in public spaces—especially while using your device

Upon Return

Upon return to the United States, wipe all personal devices to remove any malware that may have been placed on your devices.

If you have traveled abroad for business with state-owned equipment, contact the security team to investigate your work device(s) for threats and malware.

Revision Table

Date	Authored by	Approved by	Version	Notes
07/05/2022	NDIT GRC	NDIT Management	1.0	Creation of International Traveler Guidelines
06/15/2023	NDIT GRC	NDIT Management	1.1	Annual Review
10/27/2023	NDIT GRC	NDIT Management	1.2	Changed employee language to team member
11/06/2024	NDIT GRC	NDIT Management	1.3	Annual Review
08/18/2025	NDIT GRC	NDIT Management	1.4	Annual Revisions, updated language and resource links