## Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other state agencies is encouraged to the extent allowed by law.

## Responsibilities

All covered personnel are accountable for the accuracy, integrity, and confidentiality of the information to which they have access. All covered personnel that utilize IT resources while travelling internationally are responsible for adhering to this policy.

| Role | Definition |
|---|---|
| **Information Security Officer** | The Agency Security Liaison, Information Security Officer (ISO), Chief Information Officer (CIO), or other designated organizational officials at the senior leadership level are assigned the responsibility for the continued development, implementation, operation and monitoring of International Travel security requirements. |
| **Agency Management** | All levels of management must ensure employees, contractors, and vendors adhere to approved information security procedures by ensuring staff are informed about their security responsibilities and attain continued education relevant to information security and their position in the organization. |
| **Covered Personnel** | Covered personnel are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of compromise of information or information systems managed by the State. |
| **Third Parties** | Third party service providers must comply with State International Travel requirements when travelling internationally on behalf of the State. |

# Policy

The State of North Carolina has established requirements under which covered personnel may be permitted to travel with electronic devices when conducting State business or when otherwise representing the State. Each individual is required to comply with the terms of this policy before traveling outside of the United States in order to safeguard the State's data and assets.

The State has adopted the security principles established in NIST SP 800-53. The following subsections in this document outline the International Travel requirements that each agency must develop or adhere to in order to be compliant with this policy.

# Potential Risks

Traveling with electronic devices outside of the United States increases the risk that sensitive information (Restricted or Highly Restricted Data) may be exposed, or the device may become infected with malicious software (malware). This risk is especially high when governments operate and manage Internet connectivity, or the device is out of the control of the traveler.

Individuals intending to travel outside of the United States shall contact NC Department of Information Technology (DIT) prior to taking state-owned devices out of the country in order that the necessary precautions may be taken to reduce the likelihood that the device(s) will be compromised and reduce the impact if compromised. This is especially important when traveling to high risk countries as identified by U.S. State Department. This information may be found via the following link: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html.

# General Guidelines

1. **Obtain Approval to remote access State infrastructure**

   When traveling overseas for work, it is mandatory to ensure that DIT Enterprise Security and Risk Management Office (ESRMO) is alerted of your travel plans. Employees are required to submit a ServiceNow ticket that includes approval from an agency supervisor and/or agency security liaison, country of travel and duration. DIT ESRMO monitors all international connections into the State infrastructure and will terminate any connections, e.g. VPN, from overseas locations that were not pre-approved.

2. **Take only what you need**

Only take the electronic devices (laptops, smartphones, tablets, cell phones, etc.) that you need for your trip. Individuals should take only those mobile devices with them that are necessary to accomplish the mission requirements. Leave any unnecessary electronic device(s) at home.

3. **Assume everything you do on your devices will be intercepted**

The information that you send over a network may be monitored, even when using a hotel or business connection. It is always best to assume you are being monitored so that you can adjust your actions accordingly. It is highly recommended that you do not conduct financial transactions or other sensitive work while you are travelling abroad.

If you must conduct legitimate business of a sensitive nature, use a State approved virtual private network (VPN) connection before logging into any websites or accessing sensitive data, if VPN use is available and legal where you are travelling.

4. **Encrypt all data on all devices**

All data shall be encrypted on all mobile devices at all times (e.g., laptops, USB drives, etc.). It is extremely important to encrypt data while traveling and it is often easier and safer to encrypt all information as opposed to identifying the restricted information and encrypting only that information. Refer to the System and Communications Protection (SC) Policy requirements, SC-12 and SC-13, for more information.

5. **Never use public Wi-Fi, computers, or devices**

Shared computers in cyber cafes, public areas, hotel business centers, and foreign institutions-as well as devices that belong to other travelers-should never be used to access the State network or personal systems that are protected by a username and password. Public, free Wi-Fi connections cannot be trusted and may compromise your device if you attempt to connect to them.

Do not access sensitive accounts or conduct sensitive transactions over public networks, including hotels and Internet cafés. If a connection to sensitive accounts or systems is required use a virtual private network (VPN), if it is legal in the country in which you are traveling. A VPN ensures that all communication between the portable device and a State application is encrypted.

6. **Keep your device with you at all times**

Do not leave your devices out of your sight. Should customs or other airport officials take your devices out of your view, those devices should be considered compromised and should not be used. Even if you will not be using your device, it should not be left in a hotel room, conference center, or foreign office unattended. Never store devices in checked luggage. If you are unable to keep your device(s) with you, remove all battery sources from the device(s).

**7. Do not use unknown storage devices**

Portable storage devices, such as USB drives, can be used to install malicious software on your devices and allow unauthorized individuals to compromise your data and accounts. Only use those devices that you have brought with you. Public charging stations at airports or hotels should also be avoided, as they can transmit harmful software to your devices.

**8. Be aware of your surroundings**

When entering your username and password into your devices, be aware of those around you. Someone may be closely watching your screen and keyboard in an attempt to steal your credentials.

**9. All devices should be erased and rebuilt upon your return**

Have laptops, cellphones, and portable devices sanitized *prior* to travel. All devices with which you traveled should be considered compromised upon your return. They could contain malicious software that you do not want to introduce to the State's network or to your home network. Have those devices securely erased and rebuilt, either from an existing backup or through a new installation of the operating system.

**10. Change your passwords**

*Before traveling*, change all passwords that you will use and change them again upon return. You must change your password for all services that you have accessed while abroad. This should be done for your state accounts as well as any personal accounts – email, social, or financial sites – that you accessed while traveling. By limiting the sites you visit while abroad, you reduce the number of passwords you need to change. If possible, request temporary accounts to be created and deleted upon return.

**11. Report any suspicious events upon return**

*After traveling,* report any suspicious activities to your agency's security liaison such as occasions when your device was out of your control for a period of time or anomalous behavior of endpoint devices. Ensure you do not immediately connect state or personal devices to work or home networks. It is recommended that users change their passwords upon re-entry into the country.

## Laptops

**1. Use of State issued devices**

Agency management should issue specially configured devices with additional security controls to individuals before they travel to risky locations, which are in accordance with agency policies and procedures. When possible, travel with a new or reimaged device so that no data is stored on it. Contact DIT or your agency's desktop support group for loaner devices. These devices are usually supported but subject to availability. Loaner devices provide the following benefits:

- No long-term storage of sensitive information
- Limits access only to information pertinent while on travel
- Ability to wipe and reset the device upon return

**2. Remove any Restricted or Highly Restricted data**

Prior to travel, remove any restricted or highly restricted data from your laptop. This includes personally identifiable information (PII), financial information, proprietary information, agency business or planning documents, and any other materials or information that should not be made public. Materials related to the travel arrangements, presentations, supporting materials, educational information, and any other public domain documents can reside on the laptop.

**3. Uninstall applications that you do not need**

Keep on the laptop only those applications that are necessary for your travel. Uninstall any applications that you do not need or do not use. For those applications that remain, ensure that they are up to date with the latest security patches. This is especially important for those applications that interact with the web, including web browsers, Adobe Acrobat and Flash, Silverlight, and Java. Be aware that United States Export control laws preclude bringing some software applications across the borders of many countries.

**4. Keep the Operating System up to date**

The laptop's operating system, whether it is Microsoft Windows, Apple OSX, or some version of Linux, should have all the latest security patches applied to it.

**5. Verify anti-virus software is up to date**

Ensure the latest version of endpoint protection is installed on the laptop and confirm that the virus definitions are up to date.

**6. Update the settings on your web browsers**

All web browsers should be set to automatically clear the browsing history and cache after each session. Contact the DIT Service Desk for assistance in applying these settings to your preferred web browser.

## Cell Phones and Mobile Devices

1. **Consider not using a smartphone**

   Mobile phones have become mini-computers and generally contain all of our email, private communications, and contact lists. These are high-value targets for international cybercriminals. The safest course of action when traveling abroad is to procure a non-smartphone that will be used only for making calls.

2. **Back up and reset your device**

   If you will be traveling with a smartphone or mobile device, you should back up the device and then reset it to its factory default setting. This will clear all personal information from the device and allow you to selectively copy certain information back on to the device. Upon return, your device can then be restored to its previous state.

3. **Limit data contained on the device**

   Email and contact lists contained on cell phones are often filled with information that international cybercriminals covet. Email can contain non-sensitive but highly confidential information. When traveling, it is best to remove from your device any email accounts, including your State email account and any personal accounts. At a minimum, the contacts and amount of email synced to your devices should be limited to what you absolutely need while abroad.

   In addition, delete any saved, bookmarked, or favorite sites that could expose personal information or browsing habits. Remove any private data, pictures, and information that could be used to identify you or your work.

4. **Use Biometrics or strong passcodes**

   Use biometrics, strong passwords, passphrases, or passcodes to protect cell phones and mobile devices. This will prevent others from picking up your devices and gaining access to them.

5. **Disable Bluetooth and Wi-Fi**

   Turn off all device network connections and services until they are needed. Unless you are actively using these features, you should disable them on your phone or other mobile devices. Allowing these services to run provides potential attackers with a method for gaining access to your device.

6. **Install Anti-Malware or Mobile Threat Defense Application**

   Similar to computers, cell phones are susceptible to malware attacks. It is important to protect the data on your mobile phones by using solutions that will detect and prevent malware from hijacking

and compromising the data on your phone. Additionally, if the device is a State-issued or stipend phone, ensure that the State's mobile device management (MDM) or mobile application management (MAM) service is installed to ensure State data is protected. These applications will allow the data to be erased remotely should the device be stolen or lost.

## DIT Service Desk Assistance

**Inventory Your Equipment**

The DIT Service Desk can inventory your equipment prior to your travel. This will allow DIT to assist you in reporting lost or stolen devices, should you need to do so while traveling. DIT can then also verify the state of your operating system and applications.

Inform the supporting desktop support when traveling to areas considered high risk for data exploitation. The Enterprise Security and Risk Management Office (ESRMO) working with local FBI and DHS liaisons can provide more details on these countries. When traveling to these high-risk countries and communication back into the State network is required, users should request specially configured, "clean" devices, if available. These devices must not be added to the State network upon return

Users must also ensure that any loss, theft or compromise of these devices prior to, or during the travel, be reported immediately. Report any lost or stolen devices to the American Embassy or Consulate in the country you are visiting. Also, report any lost or stolen devices to NCDIT via the Statewide Cybersecurity Incident Report form: https://it.nc.gov/resources/cybersecurity-risk-management/nc-information-sharing-analysis-center/statewide.

**Monitor your accounts**

When notified of your travel dates, your agency helpdesk should monitor the logins from your State account to look for any anomalous behavior. Should DIT identify any suspicious behavior associated with your account, they will contact you immediately to change your password.

## Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

## Material Superseded

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

## Appendix

The following guide is provided by the Overseas Security Advisory Council (OSAC), which is a Public/Private Sector partnership authority of the U. S. Department of State.