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 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 traveling 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 they are informed about their data protection and 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 and/or owned by the State.
Third Parties	Third party service providers must comply with State International Travel requirements when traveling 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. Each individual is required to comply with the terms of this policy before, during and returning from travel 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 information (including 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.

Covered personnel intending to travel outside of the United States for State Business shall submit a security exception request (Form C) to NC Department of Information Technology (DIT) prior to taking state-owned devices out of the country. This is to ensure necessary precautions are taken to reduce the likelihood of State resources and data being 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.

State Owned Laptops and Mobile Devices

Use of State Issued Devices

Always encrypt data stored on mobile and external storage devices (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.

Primary State **laptops** shall not be taken for international travel. Before personnel travel internationally for approved State business, agency management shall issue specially configured laptops with additional security controls to personnel, which are in accordance with agency policies and procedures.

Primary State issued **mobile phones** that are enrolled in a mobile device management or mobile application management State platform (e.g., InTune) can be taken for international travel supporting approved North Caroline State business.

Personnel traveling internationally for approved State business shall contact DIT or their agency's desktop support group for loaner devices. These loaner devices are usually supported but subject to availability. Request for loaner devices should occur *at least 4 weeks prior to the travel date*.

Loaner devices shall provide the following configuration:

- No long-term storage of sensitive information, all information should be saved to OneDrive, not on laptop hard drives.
- Limit access to only authorized personnel
- Limit access only to information pertinent while on travel
- Allow installation of only those applications necessary to conduct State business
- Ability to wipe and reset the laptop upon return

International Travel for Non- North Carolina State Business

Carrying State-owned devices (cell phones, tablets and computers) during personal international travel (not on behalf of the State of North Carolina) is prohibited. This measure is necessary to mitigate the risks of unauthorized access to State systems associated with international travel, including the potential loss, theft, inspection, or confiscation of devices that contain sensitive information.

If personnel must access the State's network during personal time off while traveling, meaning the travel is not official State business, the personnel's manager must submit a security exception (Form C) to DIT ESRMO with the Agency's CIO approval *at least 4 weeks prior to travel dates*. Personal devices will have to be managed via the Agency mobile device management (MDM) or mobile application management (MAM) platform to access State applications, including email. The use of virtual desktops provided by agencies to allow secure access to State applications is also an approved option.

Required 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 Business travel plans. Employees are required to submit a ServiceNow ticket that includes approval from an agency Information Security Officer, 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, tablets, mobile phone, etc.) that are needed for the trip. Personnel should take only those 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 required that all business conducted use a State approved virtual private network (VPN) connection before logging into any website or accessing sensitive data, if VPN use is available and legal where you are traveling.

4. **Never use public Wi-Fi, shared 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-must not be used to access the State network. 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 connect to the State approved 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.

5. **Keep devices with you at all times**

   Do not leave 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 a device, it should not be left in a hotel room, conference center, or foreign office unattended. Never store devices in checked luggage.

6. **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 State data and accounts. Only use those devices that you brought with you. Public charging stations at airports or hotels should not be used, as they can transmit harmful software to devices.

7. Be aware of surroundings

Be aware of those around you when entering usernames and passwords. Someone may be closely watching your screen and keyboard in an attempt to steal your credentials.

8. Change your passwords

Before traveling, personnel shall change all passwords that will be used during travel and change them again upon return. Personnel must change passwords for all services that were accessed while abroad. This should be done for state accounts and is a recommended practice for any personal accounts – email, social, or financial sites – that were accessed while traveling. By limiting the sites visited while abroad, personnel can reduce the number of passwords that need to be changed.

11. Report any suspicious events upon return

After traveling, personnel shall report any suspicious activities to their agency's security liaison such as occasions when a device was out of the personnel's control for a period of time or anomalous behavior of endpoint devices. Personnel shall ensure they do not immediately connect state devices to work networks.

DIT Service Desk Assistance

Inventory Equipment

The DIT Service Desk can inventory a personnel's 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 DIT Enterprise Security and Risk Management Office (ESRMO) working with local FBI and DHS liaisons can provide more details on these countries.

Users must also ensure that any loss, theft or compromise of State-owned 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/programs/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form.

Monitor accounts

When notified of a personnel's travel dates, the agency helpdesk should monitor the logins from the personnel's State account to look for any anomalous behavior. Should DIT identify any suspicious

behavior associated with a personnel's account, they will contact the personnel immediately to change the personnel's 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 is a checklist for international travelers:

1. Obtain approval from agency CIO (or delegate) and DIT ESRMO prior to travel (i.e., security exception request Form C).
2. Submit Service Now ticket to DIT ESRMO *if travel is approved*.
3. Request a loaner device from agency for approved international travel *for the State*.
4. Take only those electronic devices you need for the trip.
5. Ensure MAM is installed on any personal devices used for State business.
6. Change all passwords that will be used before AND after traveling.
7. Keep all devices secure and with you at all times.
8. Report any suspicious activity or loss that occurred while traveling.