	State of Connecticut **Office of Policy and Management**		
Policy Title:	**Foreign Travel Policy**		
Policy ID:	IT-SEC-17-03		
Version:	1.00		
Date Issued:	11/14/2017	**Date Effective:**	11/14/2017
Last Review:	N/A	**Next Review:**	11/14/2019
Scope:	Executive Branch Agencies	**Authority:**	C.G.S. § 4d-8a
Summary:	This policy defines the steps and actions a state employees must follow when using state-owned or state-authorized electronic devices when traveling internationally and provides guidelines for state agencies whose employees may engage in foreign travel.		

Purpose

This policy defines the requirements and provides guidance for state employees traveling internationally with state authorized electronic devices.

Scope

This policy covers all State of Connecticut Executive Branch employees and interns whether permanent or non-permanent, full, or part-time (hereafter collectively referred to as "users") who access or use the state systems with a state authorized electronic device in the performance of their assigned duties.

This policy applies to all State of Connecticut Executive Branch agencies with a department head as defined in C.G.S. § 4-5. This policy does not apply to the Judicial or Legislative Branches of government, State institutions of higher education or Quasi-Public agencies as defined in C.G.S. § 1-120. However, these branches or Quasi-Public agencies may consider adopting any or all parts of this policy.

Authority

In accordance with C.G.S. § 4d-8a, the Office of Policy and Management ("OPM") is responsible for developing and implementing an integrated set of policies governing the use of information and telecommunications systems for state executive branch agencies.

Policy Statements

1. As necessary, agencies may establish or impose additional restrictions related to this policy that may be in the best interests of the agency. Any agency imposing additional restrictions must do so by written policy, a copy of which must be provided to OPM and distributed to the affected employees, prior to the effective date of that agency policy. No agency policy may be less restrictive than this policy. The Director of Human Resources (or person serving in this capacity) within each State agency is responsible for addressing individual employee questions concerning this policy

2. Extra consideration must be taken when traveling outside the United States with electronic devices, particularly if such devices will be used to connect to an Internet connection or cellular data network while abroad. Concerns range from basic theft of belongings to targeting of electronic data. Expect that your electronic devices will be compromised. It is important to prepare properly and use appropriate safeguards while traveling and upon return to the United States. The guidelines and recommendations listed below outline and define steps you can take to protect yourself, state data, state electronic devices, and personal electronic devices, or both, that contain state data.

3. If possible, do not take electronic devices with you.

4. If you must take an electronic device, consider using a state authorized temporary device, such as an inexpensive laptop and/or a prepaid cell phone that cannot connect to the Internet and is purchased specifically for travel.

Follow these guidelines if you will be taking an electronic device on the trip

Before You Go

- Backup your device.
- Once travel authorization has been approved, the DAS/BEST helpdesk must be advised by the agency that international travel is occurring.
- Be sure that any device with an operating system and software is fully patched and up-to-date with all DAS/BEST authorized security software.
- Ensure that automatic logins, the push/pull of data, and auto-download features are disabled. Turn off all other device network connections and services when not in use.
- Clear browsing histories and other stored information that could be abused. Delete unnecessary applications, plugins, and software.
- Be sure to password or passcode protect the device. Do not use the same passwords/passcodes that you use on your work and personal devices. The password/passcode should be long and complex.
- Encrypt data storage and conduct all activities over encrypted connections, if it is legal in the country where travel is occurring.

- Minimize the data and applications installed on laptops to only that which is required for business.
- Where possible use a one-time, temporarily assigned state email account instead of regularly used state email accounts.
- Know the local laws regarding online activity, as some online activity that is legal in the United States is illegal in other countries. Consult the State Department website for information about particular destinations.

During Your Trip

- Assume that anything you do on the device, particularly over the Internet or cellular data network, will be intercepted. In some cases, encrypted data may be decrypted.
- Where possible, use wired connections instead of cellular, Bluetooth or Wi-Fi connections.
- Do not use shared computers in cyber cafes, public areas or hotel business centers to access state networks, such as email.
- Never use devices belonging to other travelers, colleagues, or friends to conduct any state business.
- Use a Virtual Private Network (VPN) to access State resources.
- When not in use, turn off the device(s). Do allow them to be in "sleep" or "hibernation" mode when they are not in active use.
- **Do not** accept USB thumb drives or other removable media from any source.
- **Do not** plug USB powered devices into public charging stations, as the charging station may transfer malware to or download data from the device. Only connect USB powered devices to the power adapter with which they were intended to be used.
- Keep the device(s) with you at all times during your travel. Do not assume they will be safe in your hotel room or in a hotel safe.
- Immediately report suspicious activity, including incidents in which your electronic device is handled or examined by anyone, lost or stolen to the DAS/BEST helpdesk.

Upon Your Return

- Discontinue use of the device(s). The hard drive of the devices should be reformatted, and the operating system and other related software reinstalled, or the device properly disposed of.
- Change any and all passwords you may have used abroad.

Compliance

Agency Heads are responsible for ensuring compliance with this policy and may appoint a responsible designee from within their agency for policy oversight and administration.

Compliance with this policy is subject to audit by the Auditor of Public Accounts.

Implementation

The State's Chief Information Officer is responsible for developing and disseminating standards and planning guidelines governing the implementation of this policy. Such

standards and planning guidelines are therefore considered an extension of this policy and compliance is required thereto.

Definitions

Electronic Device	Includes any state-owned cellular phone, smart phone, Blackberry, tablet, laptop or other similar portable device including personal devices with Good for Enterprise Software.

Additional Resources

Policy on Security for Mobile Computing and Storage Devices – http://www.ct.gov/opm/cwp/view.asp?a=3006&q=561694