CONNECTICUT
Policy and Management

Policy Title:	Policy for Travel with State Information Technology Assets
Originator:	Office of Policy and Management ("OPM")
Effective Date:	February 20,2026
Supersedes:	Foreign Travel Policy, IT-SEC-17-03 v. 1.0 (11/14/2017)
History:	Version 2.0
Applies to:	State Agencies defined in C.G.S. § 4d-1(3)
Relevant Laws or Regulations:	C.G.S. §§ 4-5, 4-8, 4-65a, 4-66, 4d-1(3), and 4d-8a.

Purpose

The purpose of this policy is to reduce the cybersecurity and counterintelligence risks to State of Connecticut information, systems, personnel, and mission operations during travel.

This policy defines the requirements and provides guidance for users of Connecticut state information technology assets traveling internationally or to non-continental United States territories with state-owned or state-authorized electronic devices. This policy provides obligations and guidelines for state agencies whose employees engage in covered travel.

Enabling Authority

In accordance with Connecticut General Statutes ("C.G.S.") §§ 4-5, 4-8, 4-65a, 4-66, 4d-1(3), and 4d-8a, the Office of Policy and Management ("OPM") is responsible for developing and implementing an integrated set of policies pertaining to information and telecommunications systems for state agencies.

Scope and Reach

This policy applies to state agencies defined in C.G.S. § 4d-1(3) and covers all employees, contractors, interns or other individuals whether permanent or non-permanent, full, or part-time (hereafter collectively referred to as "users") who engage in covered travel and either access or use state systems with state-owned or state-authorized electronic devices.

Covered travel includes:

- Any travel outside of continental United States; and
- Any work conducted from non-continental United States, foreign soil, including conferences, training, site visits or telework while abroad.

Covered assets include:

- State or agency furnished electronic devices, such as laptops, tablets, smartphones, removable media, authentication tokens and any device that can access state systems or store state data.
- Personal electronic devices used for official state business or used to access state systems while engaged in covered travel.

This policy is governed by the State of Connecticut Information Security Policy and subject to the definitional and functional requirements outlined in the most recent version of that policy. The State of Connecticut Information Security Policy defines the mandatory vs. recommended requirements (SHALL vs. SHOULD) as used herein, Roles and Responsibilities, and related approval or notice requirements for Agency-level policy deviations or exceptions from this policy.

Other branches of government, including the Legislature and the Judiciary, are encouraged to adopt similar standards. State agencies working under an optimization Memorandum of Understanding ("MOU") with the Department of Administrative Services ("DAS") should engage with the Bureau of Information Technology Solutions ("BITS") to support the development, maintenance and implementation of appropriate agency-level implementation of this policy, if needed, in support of this statewide policy. Such implementation may be specific to an agency, or common among similar agencies (particularly those under an optimization MOU).

Policy Statement/Narrative

Users shall not travel with state-issued electronic devices or access state systems or data to or from countries listed on the U.S. State Department's Level 4 List, as amended from time to time. If you must travel for work related activities to a country on this list, please contact the DAS/BITS Chief Information Security Officer (CISO) office to discuss technology options.

For other covered travel, if possible users should not take state-owned or state authorized electronic devices with them.

If state-owned or state-authorized electronic devices are taken, users should otherwise employ the best practices detailed below to minimize the associated risks.

Users should anticipate that electronic devices will be compromised. It is important to prepare properly and use appropriate safeguards while traveling and upon return to the United States.

Before You Go

Users should:

- Take only the minimum information or computing hardware you need, including sensitive information contained on electronic devices. Consider the consequences if your information were to be accessed by a foreign adversary or malicious actor.

Users shall:

- Backup your electronic devices before departing for covered travel.
- Follow established agency travel authorization requirements. Submit an Office 365 International Travel request via Helix or contact the DAS-BITS Help Desk by telephone at 860-622-2300 during normal business hours **no less than 15 business days prior to approved travel**.
- Complete any DAS-BITS assigned security training or educational requirements prior to travel.
- Ensure all electronic devices are fully patched.
- Upgrade all installed software & applications to the most recent versions.
- Ensure that all electronic devices and hard drives/storage devices are encrypted; Laptops must have BitLocker or equivalent encryption enabled.
- Ensure that automatic logins, saved/autocomplete passwords, the push/pull of data, and auto-download features are disabled.
- All electronic devices must have Multi-Factor Authentication ("MFA") enabled with a passphrase, biometric or alphanumeric code required before granting access.
- Passphrases (not just passwords) must be unique to each device.
- Users are responsible for knowing the local laws of the destination country regarding online activity, as some online activity that is legal in the United States is illegal in other countries. Consult the U.S. Department of State website for information about particular destinations.

During Your Trip

Users shall:

- Maintain physical possession of your electronic devices at all times. Do not check electronic devices in airline luggage.
- Do not leave electronic devices or sensitive information unattended. A hotel safe is never "safe." If you must leave an electronic device unattended, power down the device.
- Assume that anything you do on the electronic device, particularly over the Internet, WiFi or cellular data network, will be intercepted. In some cases, encrypted data may still be decrypted.
- Do not use shared computers in cyber cafes, public areas or hotel business centers to access state networks or systems, such as email.
- Never use electronic devices belonging to other travelers, colleagues, or friends to conduct any state or personal business.
- Always use a Virtual Private Network ("VPN") to access state resources.
- Make use of digital signature and encryption capabilities of your electronic device when possible.
- When not in use, turn off the electronic device(s), or put them in "hibernation mode." Do not allow your electronic devices to be in "sleep" mode when not in use.
- Do not accept or connect USB thumb drives or other removable media from any source.
- Do not plug USB powered electronic devices directly into public USB 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.
- If a customs official demands to unlock or examine your electronic device, or if you suspect your hotel room was searched while the electronic device was in the room and you were not, assume the device has been compromised. As soon as possible:
    - Report the incident to DAS-BITS Help Desk;
    - Notify your agency leadership; and
    - Treat the device as potentially compromised thereafter.

Upon Your Return

Users shall:

- Change any and all passwords on your electronic devices you may have used abroad.

- Change your mobile device and your mobile phone passcodes.
- Restart your electronic devices.
- Re-authenticate with your MFA to state accounts.
- Change your Office365 password and any other passwords used to access state websites or resources.
- Discontinue use of the temporary electronic device(s) and return the device to DAS-BITS.

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.

Definitions

Electronic Device - Includes any state-owned or state-authorized cellular phone, smart phone, tablet, laptop or other similar portable device including personal devices used to access State of Connecticut systems or data.

Additional References

This policy aligns with:

- National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev.5 control families
- National Security Agency (NSA) Mobile Device Best Practices When Traveling OCONUS
- Federal Mobility Group (FMG) International Travel Guidance for Mobile Devices
- NIST Cybersecurity Framework (CSF) 2.0

Version History

Date	Version	Description	Publisher
Nov. 14, 2017	1.0	Initial Policy; (Foreign Travel Policy, IT-SEC-17-03)	Office of Policy and Management
Feb. 20, 2026	2.0	Update to processes, scope and best practices	Office of Policy and Management