Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

STATE INFORMATION SECURITY FOREIGN TRAVEL POLICY

Version 1.1

Date Issued: December 14, 2023

Date Last Revised: December 13, 2023

Maryland Government
Department of Information Technology
100 Community Place
Crownsville, MD 21032

Table of Contents

List of Tables

Revision Control History

Date	Reason for Change	Changed by	Version
11/1/2023	First Draft	Office of Security Management	DRAFT
11/21/2023	Version 1 DRAFT Completed	Office of Security Management	1.0
12/12/2023	Version 1 DRAFT Review Completed	Office of Security Management	1.0
12/13/2023	Version 1.1 DRAFT Completed	Office of Security Management	1.1

Table 1: Revision Control History

Approval

State CISO Gregory Rogers

12/13/2023
Date

1. Executive Summary

This policy defines the steps and actions a state employee 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.

2. Purpose

This policy defines the information security requirements and provides guidance for state employees traveling internationally with state authorized electronic devices. This policy outlines the different requirements of personal travel and business travel, as well as the approvals needed for exceptions.

3. Scope

This policy applies to each agency or unit of the Executive Branch of State government ("unit of State government").

4. Authority

- Section 3.5–2A–04 of SB812, Ch. 242 (2022)

5. Policy

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.

Unless authorized, do not take state-issued electronic devices with you, and do not connect to State systems while traveling outside the United States.

Travel to Canada is exempt from this policy restriction, but all state-issued devices must adhere to State information security requirements in the State Information Technology Security Manual. This manual can be found on the OSM website located at:

https://doit.maryland.gov/cybersecurity/Pages/policies-and-guidance.aspx

When traveling to foreign locations in support of approved State business, employees will travel with approved state-issued equipment required for business purposes. All state-issued equipment will adhere to the following requirements as set forth in the State Information Technology Security Manual, Control CM 2.7, if foreign business travel is approved by the authorizing officials:

- No personally owned mobile devices will be used on foreign travel to perform government related work.
- Only Agency approved and furnished mobile devices are allowed.
- Approved foreign travel devices including any removable media must be configured to encrypt stored data using FIPS 140-2 validated encryption.
- Device must provide protection against malware.
- Travelers must ensure physical security of the device while in transit and while on foreign travel or foreign duty.
- All devices must be reviewed for sensitive data (e.g., Personal Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Criminal Justice Information (CJI), or sensitive state business data) and this data shall be removed from the device.

6. Loss of Device or Security Compromise

Employees who experience a loss, theft or compromise of state-issued mobile computing devices (e.g., laptops, tablets, smartphones, etc.) or other electronic communication, computing, or data storage equipment shall immediately report the loss to their Agency Incident Response Team (IRT). The Agency IRT shall contact the Maryland Office of Security Management (OSM). The Agency IRT will work with OSM and General Counsel to determine if there was a loss of state sensitive data (e.g., PII, PHI, FTI, CJI, or sensitive state information). This applies to lost, stolen, destroyed, or devices for which physical control and possession has been lost.

If a user knows of or suspects that a device, information, or system has been compromised in any way, the compromise must be reported immediately to the Agency IRT and DoIT Service Desk.

7. 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.

Travel within the United States and Canada is exempt from this policy. Travel within the United States with state-issued equipment is subject to all applicable information security policies and standards.

8. Exemptions

Exemptions to this policy must be requested in writing to the Agency Head and the request shall be escalated in writing to the State CISO for final approval. Only the State CISO may approve exemptions to this policy.

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 OSM and distributed to the affected employees, prior to the effective date of that agency policy. No agency policy shall be less restrictive than this policy.