Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

STATE INFORMATION SECURITY FOREIGN TRAVEL POLICY

Version 2.1

Date Issued: January 24, 2025

Date Last Revised: January 24, 2025

Table of Contents

Revision Control History

Version	Author	Date	Description
1.0	Office of Security Management	11/2/2023	First Draft
1.0	Office of Security Management	11/21/2023	Version 1 DRAFT Completed
1.1	Office of Security Management	12/12/2023	Version 1 DRAFT Review Completed
2.0	Office of Security Management	12/13/2023	Version 1.1 DRAFT Completed
2.0	Office of Security Management	10/28/2024	Version 2.0 DRAFT Completed
2.0	Office of Security Management	10/13/2024	Version 2.0 FINAL Completed
2.1	Office of Security Management	1/24/2025	Version 2.1 FINAL Completed

Approval

Jason Silva 1/24/2025

Jason Silva — Date

Acting State Chief Information Security Officer

Purpose

This policy establishes the information security requirements and provides guidance for State employees and contingent workers traveling internationally with State issued electronic devices. The process that must be followed when traveling with State-issued electronic devices is defined below. This policy outlines the different requirements applicable to personal travel and business travel, as well as the approvals needed for exceptions.

1. Scope & Authority

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

- SF&P § 3.5–2A–04
- SF&P § 3.5-303

2. Policy

Extra consideration will 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 or connection may be compromised. It is important to properly prepare and use appropriate safeguards while traveling internationally and upon return to the United States.

Authorized Travel Locations

All travel outside the US (except to Canada), where the user intends to bring a State-issued device or access State systems or information, must be reported in advance to DoIT through the DoIT Service Desk. It is the responsibility of the user to ensure that all security requirements are met. It is highly recommended users coordinate with DoIT or their agency IT support to verify their device's security.

Check the US State Department travel advisories to determine the Travel Advisory Level of the country of travel and the corresponding travel and security requirements. See Appendix A at the end of this document for more information about Travel Advisories.

Security Requirements

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 must adhere to the following requirements, based on travel location and set forth in the Location Based Requirements section of this policy, as set forth in the State Information Technology Security Manual, Control CM 2.7:

- No personally owned mobile devices may be used on foreign travel to perform government related work in countries under Travel Advisory Levels 2-4.
- Only State approved and issued mobile devices, as described below, are allowed for countries under Travel Advisory Levels 2-4.
- Travelers must ensure physical security of devices while in transit and while on foreign travel or foreign duty.
- All devices must provide protection against malware. DoIT will install DoIT's Managed Detection and Response (MDR) solution on the device if no protection is currently implemented on the device.
- All devices must be enrolled in State approved mobile device management (MDM) where technically feasible.
- Google Advanced Protection Program (APP), Microsoft 365 Advanced Threat Protection (ATP), or equivalent technology is required for certain locations based on Travel Advisory Level, set out in the following section.
- All devices and apps must be fully updated and patched. No known vulnerabilities may be present on devices at time of travel.
- All devices (e.g., laptops, phones) and apps containing State data must be configured with either Full Disk Encryption or encrypted containers to safeguard State data , as is technically feasible based on the device type.
- 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.

Location Based Requirements

The following rules define the requirements for where State employees may bring State-issued devices, and what security controls will be implemented for those devices and the users accounts. All travel outside the US with State-issued devices will be reported to DoIT through the DoIT Service Desk. It is the responsibility of the user to ensure all security requirements are met. It is highly recommended that the user coordinates with DoIT or their agency's IT support to verify their device's security.

Check the US State Department travel advisories to determine the Travel Advisory Level of the country of travel and the corresponding travel and security requirements.

- **Travel Advisory Level 1** – The User's State Issued Devices are **Approved**
  - DoIT must be notified of travel and travel form completed
    - See the Travel Request Process section below
    - Request must be made at least 2 weeks prior to travel
  - State CISO approved endpoint protection is required
  - Device and Apps must be fully patched and updated
  - Sensitive and Confidential information should be removed from device
  - APP, ATP or equivalent protection is recommended

- **Travel Advisory Level 2** – The User's State Issued Devices are **Approved**
  - DoIT must be notified of travel and travel form completed
    - See the Travel Request Process section below
    - Request must be made at least 2 weeks prior to travel
  - State CISO approved endpoint protection is required
  - Device and Apps must be fully patched and updated
  - Sensitive and Confidential information must be removed from device
  - Loaner devices are an available option for these countries
  - APP, ATP or equivalent protection is **Required**

- **Travel Advisory Level 3** – State Issued Loaner Devices are **Required**
  - DoIT must be notified of travel and travel form completed
    - State CISO approval required prior to travel
    - See the Travel Request Process section below
    - Request must be made at least 2 weeks prior to travel
  - State CISO approved endpoint protection is required
  - Device and Apps must be fully patched and updated
  - Sensitive and Confidential information must be removed from device
  - Loaner devices for these countries are **Required**
    - The users state issued devices are prohibited from these countries
  - APP, ATP or equivalent protection is **Required**

- **Travel Advisory Level 4** – State issued devices are **Not Authorized**. Loaner devices with APP implemented may be allowed only by explicit written approval by the Maryland State CISO for critical business justifications on a case-by-case basis.

4. Travel Request Process

To notify DoIT of travel to countries under Travel Advisory Level 1, contact the DoIT Service Desk at least 2 weeks prior to travel.

To notify DoIT of travel to countries under Travel Advisory Level 2, contact the DoIT Service Desk at least 2 weeks prior to travel. DoIT will provide instructions for implementation of all required security controls.

To notify DoIT of travel to countries under Travel Advisory Level 3, contact the DoIT Service Desk at least 2 weeks prior to travel. DoIT will provide instructions for obtaining and returning required loaner devices and implementation of all required security controls.

DoIT Service Desk Contact Information: **410-697-9700** or **Service.Desk@maryland.gov**

5. 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). OSM will work with The Agency IRT to determine if there was a loss of State sensitive data (e.g., PII, PHI, FTI, CJI, or confidential or privileged information). If a user knows of or suspects 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 at the contact info above. Please write this contact information and keep it in a safe place while traveling in case your device becomes lost or unusable.

6. 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.

Unauthorized travel with State-issued devices will require the user to provide such devices to the Office of Security Management for assessment. OSM will also perform a security assessment of the user's IT accounts for indicators of compromise. The user must contact the DoIT Service Desk to coordinate delivery of devices and account assessments promptly following return from such travel.

7. Exemptions

Exemptions to this policy must be requested in writing to and approved by the Agency Head and the request shall then be escalated in writing to the State CISO for final approval. Only the State CISO, DoIT Secretary, or designee 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.

Appendix A: Advisory Levels

To see Travel Advisories for every country in the world, visit travel.state.gov/traveladvisories. Click on the color-coded world map at travelmaps.state.gov for a global view.

Levels 1-4

Many factors are considered to set the Travel Advisory level for each country. These include crime, terrorism, civil unrest, health, likelihood of a natural disaster, and current events. The Travel Advisory level reason is explained, and the safety & security concerns are described. Level 1 and 2 Travel Advisories are reviewed every 12 months. Level 3 and 4 Travel Advisories are reviewed at least every six months. A Travel Advisory will also be updated anytime there is a change in U.S. government posture, normally as it relates to ongoing security concerns.

The Travel Advisory appears at the top of each country page, with a color corresponding to each level:

Level 1 - Exercise Normal Precautions. This is the lowest advisory level for safety and security risk. There is some risk in any international travel. Conditions in other countries may differ from those in the United States and may change at any time.

Level 2 - Exercise Increased Caution. Be aware of heightened risks to safety and security. The Department of State provides more advice for travelers to these areas in the Travel Advisory. Conditions in any country may change at any time.

Level 3 - Reconsider Travel. Reconsider travel due to serious risks to safety and security. The Department of State provides additional advice for travelers in these areas in the Travel Advisory. Conditions in any country may change at any time.

Level 4 – Do Not Travel. This is the highest advisory level due to greater likelihood of

life-threatening risks. The U.S. government may have very limited ability to provide assistance, including during an emergency. The Department of State advises that U.S. citizens not travel to the country or to leave as soon as it is safe to do so. We advise that you write a will prior to traveling and leave DNA samples in case of worst-case scenarios. See **Travel to High-Risk Areas.**

Varying Levels: Levels of advice may vary for specific locations or areas within a country. For instance, U.S. citizens may be advised to "Exercise increased caution" (Level 2) in a country, while also advising them to "Reconsider travel" (Level 3) to an area *within* the country.

Risk Indicators

Advisories at Levels 2-4 include one or more established risk indicators and give specific advice to U.S. citizens who choose to travel there. These are:

- **C – Crime:** Widespread violent or organized crime is present in areas of the country. Local law enforcement may have limited ability to respond to serious crimes.
- **T – Terrorism:** Terrorist attacks have occurred and/or specific threats against civilians, groups, or other targets may exist.
- **U – Civil Unrest:** Political, economic, religious, and/or ethnic instability exists. It may cause violence, major disruptions, and/or safety risks.
- **H – Health:** Health risks, including current disease outbreaks or a crisis that disrupts a country's medical infrastructure, are present. The issuance of a Centers for Disease Control Travel Notice may also be a factor.
- **N - Natural Disaster:** A natural disaster, or its aftermath, poses danger.
- **E - Time-limited Event:** Short-term event, such as elections, sporting events, or other incidents that may pose safety risks.
- **K – Kidnapping or Hostage Taking:** Criminal or terrorist individuals or groups have threatened to and/or have seized or detained and threatened to kill, injure or continue to detain individuals in order to compel a third party (including a governmental organization) to do or abstain from doing something as a condition of release.
- **D – Wrongful Detention**: The risk of wrongful detention of U.S. nationals exists.
- **O – Other:** There are potential risks not covered by previous risk indicators. Read the country's Travel Advisory for details.

SOURCE: US Department of State, https://travel.state.gov