INTERNATIONAL TRAVEL INFORMATION SECURITY

WyIT - 3024

PURPOSE: This policy defines requirements for utilizing State-owned Information technology assets when traveling outside of the United States (U.S.).

I. APPLICABILITY

This policy applies to all Executive Branch agencies, boards, and commissions staff (collectively referred to as "agencies"). This policy is also applicable to consultants, affiliates, and temporary employees.

II. DEFINITIONS

All definitions for this policy are located in the Policy Dictionary.

III. EXCEPTIONS

Any exceptions provided to the following policy must abide by the WyIT - 3002 - Security Exception Request policy.

IV. REQUIREMENTS

Many nations do not respect personal privacy. Unlike the U.S., most other countries do not have legal restrictions against technical surveillance. State government employees are a potential high-value target for surveillance. Hotel rooms, meeting rooms, rental cars, taxis, and even commercial airlines may be subject to video and audio surveillance, along with other advanced monitoring techniques of electronic devices. Conversations may be monitored, and foreign citizens may be required to report conversations held with U.S. citizens. Business and government travelers

have reported that their hotel rooms and belongings were searched while they were away. Sometimes, no effort was made to conceal the search. U.S. travelers shall assume that all activity will be monitored, and any information accessed may be exposed.

The following requirements have been compiled to aid in awareness of threats and counteract threat actors. Following these requirements will reduce but not eliminate the risk associated with the loss of confidentiality, integrity, and availability of State information and information systems, as well as personal loss of privacy.

V. PRIOR TO DEPARTURE

- State-issued devices shall not be authorized to be taken outside the US without approval from the CIO via the service desk support team request process. Requests for use must be submitted 14 days prior to travel.
- Complete a pre-travel briefing with members of the Wyoming Information Analysis Team (WIAT). The Wyoming Office of Homeland Security (WOHS) will make arrangements for this briefing.

VI. DURING TRAVEL

- State-owned assets must be under the physical control of the state employee.
- Use of the State's authorized Virtual Private Network (VPN) solution is required when on the Internet.
- Utilizing hardware and software not owned by the State on state-owned resources (e.g., USB connection storage devices) is strictly prohibited.

VII. UPON RETURN

- Devices defined as "burners" should be powered off and returned to ETS.
- Burner devices will not be plugged in or attached to the State network in any fashion upon return.
- Complete a post-travel briefing with members of the WIAT. Arrangements for the briefing can be made through the Wyoming Office of Homeland Security.

VIII. TRAVEL ADVISORY LEVELS

Sometimes, there was no effort to conceal the search. U.S. travelers shall assume that all activity will be monitored and any information accessed may be exposed. Based on the destination country's Travel Advisory Level (detailed below), access to State agency systems and data may be restricted when outside the United States.

Authorization from the CIO is required prior to accessing any state-owned digital resources(s). Requests to the CIO must include documented security compensating controls and a business rationale for international travel. This policy also applies to systems and data used by State employees, which are supplied or managed by affiliate cloud providers or services.

1. Exercise Normal Precautions

- State Technology Requirements: Assigned state-owned technologies may be used.
- Travelers' full name and device name(s) need to be provided to the State Cybersecurity Operations Center (CSOC) through the service desk support team and ticketing request process.
- Minimum device requirements include the State's authorized solutions for full disk encryption, endpoint detection and response, vulnerability management, and data loss protection. The device will be imaged with an up-to-date/supported operating system that has been fully patched. All required third-party applications will be up-to-date/supported and fully patched.
- State's authorized VPN solution for remote access is authorized for use.

2. Exercise Increased Caution

- State Technology Requirements: State-owned technology ("burner") devices will be issued to the traveler. This includes a laptop and smartphone. Upon return, the traveler or designee will return the devices to ETS for sanitization ("wipe") or physical destruction if required.
- Travelers Full Name and Device name(s) need to be provided to the CSOC through the service desk support team and ticketing request process.
- Minimum device requirements include the State's authorized solutions for full disk encryption, endpoint detection and response, vulnerability management, and data loss protection. The device will be imaged with an up-to-date/supported operating system that has been fully patched. All required 3rd party applications will be up-to-date/supported and fully patched. The device will not contain active directory user credentials (i.e., it's not joined to the domain). Local user credentials will be configured for the device and relayed to the traveler (non-administrator access).
- State's authorized VPN solution for remote access is authorized for use.

3. Reconsider Travel

- State Technology Requirements: State-owned technology ("burner") devices will be issued to the traveler. This includes a laptop and smartphone. Upon

return, the traveler or designee will return the devices to ETS for sanitization ("wipe") or physical destruction if required.

- Travelers' full name and device name(s) need to be provided to the CSOC through the service desk support team and ticketing request process.
- Minimum device requirements include the State's authorized solutions for full disk encryption, endpoint detection and response, vulnerability management, and data loss protection. The device will be imaged with an up-to-date/supported operating system that has been fully patched. All required 3rd party applications will be up-to-date/supported and fully patched. The device will not contain active directory user credentials (i.e., it's not joined to the domain). Local user credentials will be configured for the device and relayed to the traveler (non-administrator access).
- State's authorized VPN solution for remote access will be evaluated on a case-by-case basis.

4. Do not travel

State Technology Requirements: State-owned technology resources are not authorized for this travel advisory category. This includes, but is not limited to, laptops, mobile devices, and phones. The use of technology that would allow "remote" access to state resources and data is prohibited for this travel advisory category.

IX. COMPLIANCE

Failure to comply with this policy will result in disciplinary actions through the appropriate Department of Administration and Information, Human Resources process.

REFERENCES: This policy has no supporting references to websites, other policies, or federal or state statutes.

DOCUMENT HISTORY

ORIGINAL SUBMISSION				
SUBMITTED ON	**SUBMITTED BY**	**APPROVED BY**	**APPROVED BY DATE(S)**	**EFFECTIVE DATE**
June 2024	ETS Governance, Risk and Compliance	Governor's Office	June 2024	June 2024

REVISIONS		
LAST REVISION DATE	**LAST REVISED BY**	**LAST APPROVED BY**

REVIEWS		
LAST REVIEW DATE	**LAST REVIEWED BY**	**NEXT REVIEW DATE**