INTERNATIONAL TRAVEL INFORMATION SECURITY

Policy WyIT-3024

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

I. DEFINITIONS

State-Owned Information Technology Asset: Any information technology equipment authorized, managed, and maintained by the State of Wyoming.
Service Desk: The ETS Service Desk support team can be reached via the service desk portal (https://wyoprod.servicenowservices.com/ets), by email at helpdesk@wyo.gov or by phone at +1 (307) 777-5000
Wyoming Office of Homeland Security: The Office of Homeland Security's Duty Officer can be reached via email at duty.officer@wyo.gov or by phone at +1 (307) 630-2767
Burner Devices: Temporary and/or disposable electronic devices issued by the Wyoming Department of Enterprise Technology Services (ETS)

II. APPLICABILITY

Outlined in Wyoming Statute § 9-2-2904(a)(i), this policy applies to all executive branch agencies, boards and commissions, and state personnel members, including, but not limited to; full-time employees, part-time employees, trainees, volunteers, contractors, and temporary workers. Additionally, some third parties, such as contractors or vendors, may be required to adhere, as indicated in contractual requirements.

III. REQUIREMENTS

Personal privacy is not respected in many nations. 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 their hotel rooms and belongings were searched while they were away. 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.

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

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). Arrangements for this briefing will be made through the Wyoming Office of Homeland Security (WOHS).

During Travel

- State owned assets must be in 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 is strictly prohibited (i.e. USB connection storage devices)

Upon Return

- Devices defined as “burner” should be powered off and returned to ETS
- Complete a post-travel briefing with members of the WIAT. Arrangements for the briefing can be made through the Wyoming Office of Homeland Security.

Travel Advisory Levels

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 access of any state owned digital resource(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 third-party cloud providers and 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, 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.

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, 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.

Traveler’s Full Name and Device name(s) need to be provided to the CSOC through the service desk support team, 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 based 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. Use of technology that would allow "remote" access to state resources and data is prohibited for this travel advisory category.

COMPLIANCE

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

REFERENCES

International Travel Checklist