

INTERNATIONAL TRAVEL TECHNOLOGY STANDARD

See Also:

RCW [43.105.450](#) Office of Cybersecurity
RCW [43.105.054](#) OCIO Governance
RCW [43.105.020](#) (22) "State Agency"
RCW [43.105.205](#) (3) Higher Ed
OFM Travel Policy [10.10.50.a](#)
FBI: [Safety and Security for the Business Professional Traveling Abroad](#)
FBI: [OPS Business Travel Tips Guide](#)
WaTech's [Best Practice While Traveling](#)

1. **Any computing device needing international access to state resources must meet the requirements in the [International Travel Technology Policy](#) and additional security requirements.**
 - a. Devices must meet requirements specified by the agency IT security team.
 - b. Devices must adhere to the [Encryption Standard](#).
 - c. Mobile devices must be managed with a Mobile Device Management (MDM) solution approved by WaTech as required by the [Mobile Device Usage Policy](#).
 - d. Computing devices not managed by an MDM must meet agency IT security team requirements. Devices accompanying international travel must be:
 - i. Assessed and configured following the risk-based security measures below to minimize risk prior to scheduled departure date.
 - ii. Quarantined on return and validated as safe before being allowed to reconnect to the state network.
2. **Access to state data for international travel must be protected.**
 - a. Category 3 or Category 4 data must be protected as described in the State [Data Classification Standard](#).
 - b. Category 3 or Category 4 data must be approved by the agency IT security team for use on mobile devices or laptops.
3. **Access to state resources requires risk-based security measures.**
 - a. Agencies must base access decisions on a risk management methodology that follows the [Information Security Risk Management Policy](#).
 - b. Authentication must follow requirements from the [Securing IT Assets Standard \(6.3\)](#).
 - c. The approach for each international travel scenario must include an assessment (see the [Risk Assessment Standard](#)) of risks associated with:
 - i. The targeted travel location.
 - ii. The nature and purpose of the travel.
 - iii. The technical devices and services required/desired for the trip.
 - iv. The access level and organizational responsibility of each traveler.
4. **WaTech manages connections from high-risk/unsafe countries or regions for the state.**

- a. WaTech determines whether to block cyber traffic or require additional controls from countries on the unsafe country list at entry points to the SGN, state-managed on-premises environments and the Enterprise Shared Tenant.
- b. WaTech will maintain a list of high-risk countries or regions.

REFERENCES

1. [International Travel Technology Policy](#)
2. [Encryption Standard](#)
3. [Mobile Device Usage Policy](#)
4. [Data Classification Standard](#)
5. [Information Security Risk Management Policy](#)
6. [Securing IT Assets Standard \(6.3\)](#)
7. [Risk Assessment Standard](#)
8. [Definitions of Terms Used in WaTech Policies and Reports](#)

CONTACT INFORMATION

For questions about this policy, please contact the [WaTech Policy Mailbox](#)