Arkansas State University

International Travel with Institutional Devices Guidelines

Effective Date: March 7, 2025
Revised Date: March 24, 2025

1. Purpose

For the professional development of our faculty, staff, and students and to raise the recognition of our contributions and the profile of Arkansas State University (A-State), international travel is encouraged. To safeguard A-State's institutional data, minimize cybersecurity risks, and comply with export control regulations, this document outlines procedures for faculty, staff, and students planning to travel overseas with electronic devices. This guidance provides three tiers to manage devices in accordance with institutional security best practices, as determined by Information Technology Services (ITS).

2. Approved Recommendations

Before traveling outside of the United States of America (USA), consider the purpose of the trip and determine the need to take an electronic device. Anytime a faculty or staff member or student travels outside the USA, there is an element of risk regarding personal and institutional data becoming vulnerable to security breaches. The following recommendations are in order of best practices, and A-State wants to ensure there are necessary pathways and processes in place to accommodate and encourage international travel for the continued expansion of A-State on a global scale.

(i) Tier 1: No Device Travel (Highly Recommended)

It is highly recommended that travelers leave all electronic personal or institutional devices and valuables at home if possible. This approach minimizes the risk of data theft or compromise, reduces the chance of loss, and ensures compliance with security protocols while abroad.

Benefits of No Device Travel:

- Eliminates cybersecurity risks.
- Prevents loss or theft of personal or institutional assets.
- Reduces administrative processes before travel.

If personal devices are taken on international travel, all institutional data should be removed unless prior approval is given by IT Security (employees should denote this on the International Travel Justification Form). This measure helps protect sensitive information and ensures compliance with institutional security policies. Please see section 5 for further details on personal device use while traveling overseas.

(ii) Tier 2: Travel with a Loaner Device for University Business (Preferred if Device is Necessary)

If bringing a university device is essential while traveling on university business, travelers should utilize a loaner device provided through Information Technology Services (ITS). This option is highly encouraged to secure university data and minimize risks associated with personal or other institutional devices abroad. ITS and Research Compliance in Research and Technology Transfer manage and coordinate the loaner device program.

Process for Securing a Loaner Device:

1. Request Submission: Complete the Loaner Device Request Form at least 30 days before travel.
2. Approval Coordination: Obtain necessary approvals from the supervisor and the department's Academic Dean or Vice Chancellor of the administrative department.
3. Loaner Device Pickup: Once approved, coordinate with ITS for device configuration and pickup.
4. Device Return: Return the loaner device to ITS promptly upon returning from travel.

Security Specifications for Loaner Devices:

- Pre-installed with necessary cybersecurity software (KACE [or Jamf for MacOS], CrowdStrike, Malwarebytes, and Microsoft BitLocker [or FileVault for MacOS] encryption).
- Minimal preloaded data to limit exposure in case of loss or theft.
- Device reconfiguration upon return to secure institutional data.

(iii) Tier 3: Travel with an Institutional Device (Only if Absolutely Necessary)

If it is deemed absolutely necessary to travel with an institutional device while traveling on university business (laptop, tablet, or cell phone), strict guidelines apply to ensure data and device security.

Requirements for Traveling with an Institutional Device:

1. Justification Form: The traveler must complete the Justification Form outlining the necessity of using an institutional asset abroad.
2. Approval Process: The form must be signed by the traveler’s Academic Dean (or Vice Chancellor of the administrative department).
3. ITS Security Verification: Submit the device to ITS (via a Help Desk ticket request or by e-mailing security@astate.edu) for verification at least 30 days before travel. ITS will ensure that the device is updated with the latest versions of KACE (or Jamf for MacOS), CrowdStrike, Malwarebytes, and Microsoft BitLocker (or FileVault for MacOS) encryption.

4. Final Authorization: After ITS security verification, the device may receive final approval for overseas travel.

3. High-Risk Countries (As Determined by the U.S. Department of State)

In alignment with U.S. Department of State guidelines, A-State has designated a list of High-Risk Countries where the data security threat is exceptionally high.

High-Risk Countries Guidelines

For these destinations, Tier 3 (Travel with an Institutional Device) will not be permitted to ensure optimal data security. Faculty and staff are required to select either Tier 1 (No Device Travel) or Tier 2 (Loaner Device) as their device management option.

High-Risk Cybersecurity Destinations

A-State compiles the list of high cybersecurity risk countries from several sources, including countries that are the subject of Travel Warnings by the U.S. Department of State and those that are identified as high risk by other U.S. Government sources such as the Department of the Treasury Assets Control (OFAC), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI). The list will be updated regularly.

Travel to countries with different laws and expectations is sometimes necessary but presents a unique challenge to the confidentiality of university data. The following is a list of countries representing high cybersecurity risks to A-State faculty and staff traveling abroad.

- **China, The People's Republic of**
- **Cuba (Tier 1 only)**
- **Russia**
- **Hong Kong**
- **Korea, Democratic People's Republic of (i.e., North Korea; Tier 1 only)**
- **Crimea (Region of Ukraine)**
- **Iran (Tier 1 only)**
- **Syria (Tier 1 only)**

It is highly recommended that travelers check the Travel Warnings by the U.S. Department of State ahead of travel, and to check with Research and Technology Transfer (RTT) or ITS Security to ensure the destination is not in the high-risk category.

Process for High-Risk Country Travel:

1. Verification of Travel Destination: Confirm with ITS and RTT whether the destination is on the High-Risk Country list (see above).
2. Adhere to Approved Tiers: Select either Tier 1 (No Device Travel) or Tier 2 (Loaner Device) except for any countries that are identified as unilaterally or completely embargoed countries (**Cuba, Iran, North Korea, and Syria**), in which case no technology will be permitted to be taken to those countries. Complete all necessary documentation and approvals associated with the selected tier.

Important Note: This restriction is intended to prevent data loss and ensure institutional compliance with export control regulations. High-Risk Country designations are subject to change, so travelers should verify the list before each international trip.

4. Incident Response Plan

This plan provides immediate response actions for A-State personnel traveling internationally with a loaner or institutional device in the event of device loss, confiscation by Customs Border Patrol (CBP), suspicious activity, or attempted unauthorized access.

(i) If the device is lost or stolen:

1. Attempt to retrace steps if in a secure area, ensuring safety.
2. If device recovery is not possible, immediately contact Information Technology Services (ITS; security@astate.edu) and the local embassy or consulate if sensitive data are involved.
3. Document the time, location, and circumstances of the loss.

(ii) If the device is confiscated by Customs Border Patrol (CBP):

1. Do not resist CBP personnel; cooperate fully while noting details of the interaction.
2. If feasible, politely request an official record or receipt of confiscation.
3. Contact ITS (security@astate.edu) immediately to report the event, including the time, location, and CBP officer details if available.

(iii) If suspicious activity or unauthorized access is suspected:

1. Disconnect the device from any network immediately.
2. Observe and record any suspicious details, such as unusual software behavior or unauthorized access attempts.
3. Immediately contact ITS (security@astate.edu) for further guidance and follow any instructions for securing the device.

5. Personal Devices

To further protect institutional data and minimize security risks, A-State has specific recommendations for personal device use during international travel:

1. **Avoid Business Activities on Personal Devices:**
   It is highly recommended that employees do not use any personal devices to conduct business-related activities while traveling overseas, including checking university emails or accessing other university resources.

2. **Secure Email Access on Personal Devices:**
   If accessing university email on a personal device becomes necessary—such as in emergencies or unavoidable situations—employees should use the Microsoft Outlook application, available on both iOS and Android (along with Windows and Mac laptop devices).

   This app is part of the Microsoft ecosystem and provides enhanced security features. Using the Outlook application ensures better protection of institutional data, offers A-State

greater transparency into the device, and enables IT to take security measures such as remotely locking or wiping the device if it is lost or stolen.

3. **Precautions for High-Risk Locations:**
   Employees traveling to high-risk locations should remove all business-related activities, applications, and sensitive data from their personal devices, unless prior approval is given by IT Security. If feasible, it is recommended to follow **Tier 1 (No Device Travel)** and refrain from bringing any electronic devices to high-risk countries. For unexpected or emergency situations where device use may be necessary, travelers may consider purchasing a device locally upon arrival and limit its use strictly to non-sensitive activities. This approach helps reduce security risks associated with traveling with pre-owned devices and provides a safer, temporary solution when a device is essential.

These guidelines are intended to reduce the risk of unauthorized access, data theft, and cybersecurity threats associated with personal device use abroad.

5. Compliance and Reporting

Failure to follow these guidelines may lead to disciplinary actions, as it could jeopardize university data security and compliance with export control regulations. For questions, please contact Information Technology Services (security@astate.edu) or Export Control (export@astate.edu).

6. Contact Information

- **Information Technology Services:** Patrick Jeffrey, Director of IT Security (security@astate.edu)
- **Export Control:** Jenny Estes, Director of Research Compliance (export@astate.edu)

This document is intended to support all Arkansas State University personnel in responsibly managing device security while conducting international university-related activities.