WASHINGTON STATE UNIVERSITY
Division of Academic Engagement and Student Achievement

International Travel Guidance for DAESA Employees

The DAESA InfoTech Committee has indicated that traveling DAESA employees should check with DAESA IT prior to international travel. While the Committee attempted to make the steps necessary for mitigating data security risks during international travel more palatable, the approved WSU policies from the Business Policies and Procedures Manual (BPPM) governing this matter leave no flexibility.

You can find the exact text for the policies that cover the use of personally- and WSU-owned equipment to access WSU data when traveling internationally below.

BPPM Excerpt: International Travel with Personally-owned Equipment

The following text comes from BPPM 87.11.

> INTERNATIONAL TRAVEL
>
> Many countries do not respect the personal privacy of individuals and monitor personal communications. When traveling internationally and potentially traveling to one of these countries, employees must not use their **personally-owned** (note: Emphasis is ours.) mobile devices to access institutional information systems and data. If employees require access to institutional information systems and data, business units should issue temporary devices to them, which are to be used only for the duration of their international travel.
>
> Users should not store and/or maintain institutional data on a mobile device when traveling internationally. When the employee returns from their trip, they must return the temporary device, which must be reimaged prior to being issued to another user.
>
> See the following websites for security tips for international travel:
>
> - orso.wsu.edu/export-control-regulations/
> - ora.wsu.edu/export-controls/
> - its.wsu.edu/documents/2019/01/electronic-device-security-tips-for-international-travel.pdf/

PROPOSED OPERATIONAL PARAMETERS FOR DAESA Concerning International Travel with Personally-owned Devices

- International travel includes **any** travel by any means of conveyance outside of the United States (i.e., including to bordering countries such as Canada and Mexico).
- You can use your personal equipment (phone, tablet, laptop) internationally to place and receive calls and exchange texts **ONLY**, but regardless of the device you use, you may not access WSU data—including email—even with the secure enclave installed. This is true whether you are on vacation or traveling for work.
- While there are steps WSU might take to increase security, the policy leaves it clear that those mitigative steps would remain insufficient and personally owned equipment cannot access WSU systems and data while outside of the U.S.
- Once again, do not access WSU data on your personally-owned laptop while outside of the United States under any circumstances.
- To prevent unintended access from occurring, turn off, remove, and/or disable your access to WSU systems (i.e., email) prior to departure. You can restore your access when you return.

BPPM Excerpt: International Travel with WSU-owned Equipment

While we discuss international travel with personally-owned equipment above, we must remind the reader that BPPM 87.10 governs travel WSU-owned equipment. Regarding international travel, it states:

> INTERNATIONAL TRAVEL
>
> Many countries do not respect the personal privacy of individuals and monitor personal communications. When traveling internationally and potentially traveling to one of these countries, employees should not take their WSU-issued mobile devices with them. Business units should issue temporary, travel devices to employees, which are to be used only for the duration of their international travel.
>
> Users should not store and/or maintain institutional data on a mobile device when traveling internationally. When the employee returns from their trip, they must return the temporary device, which must be reimaged prior to being issued to another user.
>
> See the following websites for security tips for international travel:
>
> - orso.wsu.edu/export-control-regulations/

- ora.wsu.edu/export-controls/
- its.wsu.edu/documents/2019/01/electronic-device-security-tips-for-international-travel.pdf/

PROPOSED OPERATIONAL PARAMETERS FOR DAESA Concerning International Travel with WSU-owned Devices

- As previously mentioned and to bring DAESA into compliance with BPPM 87.10, DAESA IT will purchase devices you can check out for working on during international travel.
- DAESA employees will not take their WSU-owned laptop or mobile device on vacations to an international destination. If an individual wants to have a device available to do some work while they are way, they must check out a temporary device from DAESA IT to have on hand.
- When all devices have been checked out at the same time, DAESA IT may, in some cases, prepare individual WSU-owned devices for travel outside of the United States. To facilitate this process, IT leaders must have access to your laptop before departure to your international destination and immediately upon arrival back in the United States.
- DAESA IT strongly emphasizes the first sentence of the second paragraph of the policy stated in BPPM 87.10: "Users should not store and/or maintain institutional data on a mobile device when traveling internationally."
- When individuals connect wirelessly, they must immediately connect to the WSU VPN because this significantly helps to secure the data being transmitted over a wireless connection.

NOTE: If you lose a DAESA-assigned device while traveling you **MUST** contact DAESA IT immediately at 1-509-335-8045, 1-509-335-8876, or ascc.tech.support@wsu.edu.

DAESA InfoTech Committee recognizes that enforcing these BPPM policies impacts productivity when outside of the U.S., but ensuring that expensive, disruptive, and problematic breaches of WSU data security are prevented is well worth any perceived tradeoff in productivity. The fact is WSU remains institutionally responsible for the protection of the data it maintains, and this responsibility takes precedence.