IT Guidelines for International Travel

**GREEN recommendations: baseline security for all travelers, foreign or domestic and Public data use**

*Before your trip:*

- Ensure data is backed up on a server, drive, or other device NOT making the trip.
- Ensure your PC is patched and the antivirus software updated.
- Disable Bluetooth and Wi-Fi on your devices, and only turn them on when in use.
- Notify IT staff of travel plans and locations; IT staff should strongly consider readying spare equipment for delivery in an emergency.

*During your trip:*

- Assume your data on any wireless network can be monitored, and act accordingly. Use UAB’s VPN, especially while on public networks and/or when accessing sensitive data.
- NEVER let anyone else borrow or use your devices.
- Do not borrow any devices (e.g. a USB drive) for use on your computer.
- Do not install any software on your PC.
- Be aware of “shoulder surfers” — anyone physically monitoring the use of your device.
- Keep your devices under your physical control or secured in a proper location when they are not. Never check devices or storage devices in luggage.

*After your trip:*

- Perform a full virus and malware scan.

**YELLOW recommendations: for travelers visiting moderately sensitive destinations and sensitive data.**

*Before your trip:*

- Ensure data is backed up on a server, drive, or other device NOT making the trip.
- Ensure your PC is patched and the antivirus software updated.
- Disable Bluetooth and Wi-Fi on your devices, and only turn them on when in use.
- Notify IT staff of travel plans and locations; IT staff should strongly consider readying spare equipment for delivery in an emergency.
- Ensure your device is encrypted (if permitted by the nation to which you are traveling).
- **NOTE:** Sensitive data CANNOT be stored on a device without encryption.
  - Password-lock auto-encrypts iPhones; Android users should manually enable encryption.
  - Laptops: Use BitLocker, PGP, or a similar tool for Windows; use FileVault on OS X systems.
  - “Sanitize” your laptop to remove any sensitive data.
    - A product such as Identity Finder can assist this process.
    - Only take data necessary for the specific trip.
    - Consider taking a temporary device such as a loaner laptop or prepaid phone.
**During your trip:**

- NEVER let anyone else borrow or use your devices.
- Do not borrow any devices (e.g. a USB drive) for use on your computer.
- Do not install any software on your PC.
- Be aware of “shoulder surfers” — anyone physically monitoring the use of your device.
- Keep your devices under your physical control or secured in a proper location when they are not. Never check devices or storage devices in luggage.
- When using shared Wi-Fi, stay connected to UAB’s VPN.
- Do not use “shared” computers at a business center or kiosk, etc.

**After your trip:**

- Perform a full virus and malware scan.
- Consider changing passwords for all services/systems you used from overseas.

---

**RED recommendations:** for travelers visiting extremely sensitive/restricted destinations and restricted data. Destinations referred to a “comprehensively sanctioned” currently include Iran, Sudan, Syria, North Korea, and Cuba. Most commercially available basic software (such as Microsoft Office) can be carried or shipped to the destination either individually or on your device without a license. This situation requires that an Information Security Exception Request be completed and approved by the Data Steward, University Compliance and Information Security prior to travel.

---

**Before your trip:**

- Contact the University Compliance Office to discuss your trip and appropriate precautions to take with devices and data.
- If traveling to a country which disallows encryption products, prepare a “loaner” device.
- NOTE: Restricted data CANNOT be stored on a device without encryption.
- Ensure your PC is patched and the antivirus software updated.
- Disable Bluetooth and Wi-Fi on your devices, and only turn them on when in use.
- Notify IT staff of travel plans and locations; IT staff should strongly consider readying spare equipment for delivery in an emergency.

**During your trip:**

- NEVER let anyone else borrow or use your devices.
- Do not borrow any devices (e.g. a USB drive) for use on your computer.
- Do not install any software on your PC.
- Be aware of “shoulder surfers” — anyone physically monitoring the use of your device.
- Keep your devices under your physical control or secured in a proper location when they are not. Never check devices or storage devices in luggage.
- When using shared Wi-Fi, stay connected to UAB’s VPN.
- Do not use “shared” computers at a business center or kiosk, etc.
- Take a loaner “dumbphone” (no data storage) instead of your smartphone.
- Shut down devices when not in use (do not use sleep or hibernate features).
• Keep your device(s) on your person at all times — remember that hotel safes may be compromised.

After your trip:

• Perform a full virus and malware scan.
• Change passwords for all services/systems you used from overseas.
• Erase and reformat the hard drive on the loaner device.
• Wipe data from a temporary “dumbphone.”