UtahStateUniversity

Cybersecurity for International Travel

BEFORE YOU GO

- Check your **destination risk level** at usu.edu/risk/international-travel/country-risk-levels
- Only take **devices or information** you absolutely need
- For Medium+ risk destinations, request a **loaner device** from servicedesk@usu.edu
- Remove **sensitive files** from your device, back them up to **Box**, and uninstall **Box Drive**
- Install **OS and app updates**; ensure **anti-malware** (Intune for Windows, Jamf for Mac) is installed and active; contact MyTech if unsure
- Enable **MFA** on all accounts (USU A# accounts already have Microsoft MFA); instructions at it.usu.edu/mfa
- Install and test **USU VPN**; instructions at it.usu.edu
- Set a strong **PIN or passphrase** (6+ characters); disable **biometrics** while traveling
- Forget saved **Wi-Fi networks and Bluetooth devices**
- Contact your **mobile provider** about international plans

WHILE ABROAD

- Keep devices with you at all times, never in **hotel safes**
- Lock your **screen** every time you step away
- Shield your **screen and keyboard** in public; consider a privacy screen
- Use **USU VPN** to access all networks
- Never plug into **public USB ports** — use your own adapter and cable
- Avoid **public computers** and internet cafes — they may log keystrokes
- Ignore unknown **USB drives, printers, or Bluetooth** invitations
- Turn off **Wi-Fi, Bluetooth, and AirDrop** when not in use
- Type **URLs** directly; don't scan random QR codes
- Don't log into **personal banking** on work devices
- **Power-cycle devices** daily

WHEN YOU RETURN

- **Power-cycle devices** before reconnecting to the USU network
- Change all **passwords** used while traveling
- Run **antivirus and malware scans**
- Re-enable **biometrics** once home
- Return any **loaner equipment** to the IT Service Desk
- Monitor **bank, email, and USU accounts** for suspicious activity for 30 days

Anything unusual?
Suspected compromise?
Do not connect the device to the USU network. Bring it to the IT Service Desk or email security@usu.edu immediately.

Traveling to a High Risk or Restricted destination? *Check at usu.edu/risk/international-travel/country-risk-levels and take these extra precautions:*

HIGH RISK *(Ethiopia, Guyana, Honduras, Nigeria, Papua New Guinea)*

Policy 5303**: Students not permitted.** Faculty/staff must submit a travel safety & risk mitigation plan to Risk Management and the Int'l Travel Oversight Committee (ITOC).

- Do not bring your **normal work device**
- Use a **loaner device**; request from servicedesk@usu.edu
- Use a **burner phone** if possible
- Assume **hotel rooms and safes** are not secure
- Do not access **personal bank accounts**

RESTRICTED *(Cuba, Russia, Iran, North Korea, Ukraine + more)*

Policy 5303**: Students not permitted.** Faculty/staff must contact USU Risk Management — USU does not offer insurance coverage to these destinations.

- Email security@usu.edu before you travel
- Follow all **High Risk destination** precautions
- Assume all **traffic is monitored** or intercepted
- **VPN and encryption** may be illegal — check before you go

⚠ **Data overrides country risk.** If you work with PII, FERPA, HIPAA, GDPR-covered EU data, ITAR/EAR export-controlled research, CUI, or human-subjects data, apply HIGH-risk precautions regardless of destination — or do not take the data at all. Leave it in Box or on USU-managed systems and access remotely via VPN only when necessary. When in doubt, contact **security@usu.edu** before you travel.

LOST DEVICE OR SUSPECTED COMPROMISE?
Email **security@usu.edu** · IT Service Desk: **servicedesk@usu.edu** · 435-797-HELP (4357) · **it.usu.edu**

Sources: USU IT Security While Traveling Abroad · USU Country Risk Levels (Risk Management) · NSF SECURE Center Travel Checklists.
Review USU Policy 5303 §2.4.2 before Medium/High/Restricted travel.

HOW TO POWER CYCLE DEVICES