✈️ Travel Approvals

All international travel must be approved through the university's official system (Emburse). Travel to destinations classified as high risk by the Texas A&M System requires additional review and elevated approval. Travelers must verify destination status on the A&M System International Travel Risk Status website before making plans.

🎓 Required Training

Travelers must complete all mandatory safety and compliance training, including:

- TrainTraq Course #2113639 – U.S. Foreign Corrupt Practices Act (required every 3 years)
- TrainTraq Course #2111728 – International Travel Safety
- TrainTraq Course #2111212 – Export Controls and Embargo Training

Additional briefings may be required for certain roles or funding sources (e.g., federally funded research under NSPM 33).

💻 Device Preparation

Using a regular university owned device for international travel is discouraged. If possible secure a loaner device from your department or Technology Services. Be aware there is very limited availability of loaner devices. If no loaner device is available:

Secure: Bring your device to Technology Services to verify the required management and security software is installed and the device us up to date. Travel only with the minimum data required.

Back Up: Securely back up essential data before departure.

Sanitize: Remove all non-essential data, especially anything Confidential, Critical, proprietary, or export controlled.

🌐 Export Controls

Before taking any university equipment, software, technical data, prototypes, or samples abroad, consult RESEC Export Controls (exportcontrols@tamu.edu) . Export licenses or special handling procedures may apply.

🔒 Security During Travel

Physical Security

- Always keep devices under direct control.
- Never leave devices in hotel rooms (even in safes), meeting rooms, vehicles, or public spaces.
- Do not place laptops or critical devices in checked luggage.

- You are responsible for the physical security of your device.

Network Security

- Avoid public Wi Fi for sensitive work.
- Use a personal or university issued mobile hotspot.
- When using any untrusted network, connect through the Texas A&M VPN.
- Use only HTTPS secured websites.

Connectivity Hygiene

- Turn off Wi Fi and Bluetooth when not in use.

Limit Sensitive Access

- Access Confidential or Critical data only when absolutely necessary.
- Be aware of local surveillance laws and restrictions.

Limit Personal Use

- Minimize personal activity on university owned devices while abroad.

Special Note for Summer Sea Term

If on Summer Sea Term leave your university computer on the ship when in port in other countries to avoid the possibility of confiscation by customs

Questions?
Contact RESEC Export Controls: exportcontrols@tamu.edu