



SPACE INSTITUTE

UT Space Institute IT Procedure: International Travel	
Version: 1	Effective Date: 08/01/2025

Purpose

To ensure data security and compliance with organizational and international regulations, all employees traveling internationally must either have their laptops encrypted by IT or borrow a pre-encrypted loaner laptop from IT.

Scope

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by The University of Tennessee Space Institute (UTSI) including its remote centers.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Procedure

Users should notify IT of any international travel at least 10 business days prior to departure by submitting a ticket to helpdesk@utsi.edu that includes the following information:

- Name
- Department
- Travel dates
- Destination(s)
- Purpose of travel
- Whether you need to:
 - Bring your existing University-issued device
 - Borrow a pre-encrypted loaner laptop or device

IT will assist users bringing their own University-issued device in ensuring that all critical data is backed up, all security updates and travel restrictions are applied, and that the device is encrypted.

For pre-encrypted loaner devices, IT will prepare the device with full disk encryption, limited user access, and pre-approved software and files.



SPACE INSTITUTE

UT Space Institute IT Procedure: International Travel	
Version: 1	Effective Date: 08/01/2025

For either existing or borrowed equipment, the user is responsible for ensuring that only work-related data is stored on the machine.

Devices will need to be brought to IT within 2 business days after the user returns from travel and IT will assist with transferring any work-related files off the device. User devices will be checked to verify there has been no tampering. Loaner devices will be wiped before reissuing.

International Compliance & Restricted Travel Notice

University faculty, staff, and contractors must not:

1. Take their assigned University desktop, laptop, tablet, phone, or other device when traveling outside the U.S. to any of the following restricted countries, without prior written approval from the University CIO:
 - Foreign Countries of Concern as defined by [42 U.S.C. § 19237](#)
 - Countries under U.S. Sanctions Programs maintained by the Office of Foreign Assets Control (OFAC) – [View list](#)
 - Countries subject to a U.S. Department of State Arms Embargo per ITAR § 126.1 – [View list](#)
 - Countries under EAR Part 746 Embargoes – [View list](#)
2. Transport Protected University Data (including but not limited to FERPA, HIPAA, research data, or other sensitive institutional data) out of the United States on any system or device without explicit prior approval from the University CIO.

Exceptions

Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

Related Policies

[IT0001 – General Statement on Information Technology Policy](#)



SPACE INSTITUTE

UT Space Institute IT Procedure: International Travel	
Version: 1	Effective Date: 08/01/2025

[IT0002 – Acceptable Use of Information Technology Resources](#)