Export Control Issues Related to International Travel for Faculty, Staff, and Students

The University of Texas at El Paso (UTEP) supports and encourages international travel in order to promote research, study abroad and international collaborations with other universities throughout the world. UTEP is also committed to doing everything possible by establishing policies and guidelines to ensure the safety and wellbeing of our faculty, staff and students.

UTEP employees are responsible for knowing how export controls apply when taking equipment, devices, software or technical data outside abroad. In most situations, licensing is not required to take UTEP owned items abroad under the TMP "tool of trade" license exception. However, items such as laptops must remain under the traveler's effective control during the trip. Additionally, information and data taken on laptops, PDA's or storage devices must qualify as public domain.

The "tools of the trade" exception does not apply to controlled technology. In other words, the Bureau of Industry and Security (BIS) would require a license to take certain technologies found on the BIS Commerce Control list (CCL), depending on the technology and the country. Also, be aware that some countries have restrictions on the types of technology that you may import into that country. If your laptop is loaded with encryption products or other controlled technology, it is recommended that you arrange to take a "clean" laptop loaded with only the typical Microsoft Office suite or similar commercially available software. In addition, technologies, software or commodities that are regulated by the Department of State's International Traffic in Arms Regulations (ITAR); and proprietary, confidential or sensitive information subject to Non-Disclosure Agreements or as a result of a research project with contractual restrictions will not be exported outside of the United States.

Travel to Sanctioned/Embargoes Countries:
OFAC regulations prohibit the university from conducting any financial transaction or providing services to any blocked or sanctioned country, individual, entity or organization, including a government agency of a sanctioned country. Travel to certain sanctioned/embargoed countries would require a license from the Office of Foreign Asset Control (OFAC), or could, in fact, be denied.

Collaboration, agreements, or contracts with Foreign Entities and/or Individuals:
The Department of State, the Office of Foreign Assets Controls (OFAC), and BIS have various lists of persons and entities that we are prohibited from doing business with; in other words, we should not be providing them with a defense service (includes training), giving money to these people or organizations, or providing them with controlled technology. A restricted party screening (RPS) determines if the entities and/or individuals which whom you desire to conduct business are on any U.S. Government issued restricted, blocked or denied party lists. In addition, collaboration (e.g., presentations, discussions) must be limited to topics that are not related to research on controlled items, commodities, or technology unless the information is already published or otherwise already in the public domain. You must verify that the shared information falls into one or more of the exclusions (e.g., research that qualifies as fundamental research, information that is in the public domain, educational information, and publicly available software).

If, during travel, you are contacted by an individual or entity that wants to engage in business or have you provided other services, please contact OCRA to conduct a restricted party screening to evaluate whether the transaction can occur.

For more information about how export control regulations can affect your international travel, visit the Research & Innovation Export Controls page (Export Control (utep.edu)

UTEP policy in removing equipment from UTEP premises:
UTEP owned property may be removed temporarily from the campus and other UTEP facilities to be used in conducting official UTEP business. An "*Authorization to Remove Equipment off Campus*" form must also be completed and submitted to the Vice President for Business Affairs prior to removal from the UTEP. See University-Owned Property and Equipment Policy

Certification of Temporary Export of UTEP Property and Review of U.S. Export Control Regulations

1. **Name of Traveler:**   **UTEP Email:**

> I will **not carry UTEP-owned devices or equipment** outside of the U.S. *Please attach the form to your approval packet.*
>
> I will **carry UTEP-owned devices or equipment** outside of the U.S. Please add your devices below and sign the form. *Please attach the form to your approval packet.*

2. **Destination and Dates of Travel** (Please include foreign layover locations)**:**

Destination.	Travel Dates

3. **Purpose of Travel** (If it is for conference attendance, please provide the title and sponsor of the event);

4. **I plan to meet the following foreign individuals/entities while traveling abroad:**

Location	Name of Individual/Entity	Purpose of Meeting

5. **I am removing the following item(s) belonging to the University of Texas at El Paso:**

UTEP TAG#, MAC Address or SN	Device Host Name	Department	Device Location Building/Room #	Is Device Being Backed-up (Y/N)?

6. **Authorization to remove equipment off-campus:**

Authorization From approved by Dean, Director or Chair?	Authorization Form filed with the Department?
Yes **No**	**Yes** **No**

7. **Classification of data on device:**

Does the device contain Confidential, Research, or Sensitive Information?	If "Yes", state the level of classification (Category I, Category II, Category II, or Other (specify)?
Yes **No**	

By signature below, I certify that:

1) I have read and agreed with the UTEP policy on removing UTEP Controlled/Capital equipment from campus premises; and
2) I have reviewed the informational sheet entitled ***"EXPORT CONTROL ISSUES RELATED TO INTERNATIONAL TRAVEL FOR FACULTY, STAFF, AND STUDENTS"*** and I am aware of restrictions or sanctions that may apply to the destination and/or to the entities and individuals whom you desire to do business, if any; and
3) there is no controlled technical data or controlled technology installed or stored on any item listed above; and
4) the item(s) will remain under my effective control at all times while outside the United States and will be outside the United States for the period listed above (not to exceed one year); and
5) the item(s) will not be used by or shared with any entities on the list of restricted entities or any other person or entity subject to export prohibitions.

Traveler's Signature:	Date:

For more information on the policies, please see:
Classification of Data on Device
UTEP Information Security Policies
UT System Information Resources Use and Security Policy (UTS165)

Research & Innovation Approval indicates an export license is not required for the carrying of the above-described items outside of the U.S. and restricted party screening revealed no export concerns.

Signature:	Date:

ISO USE ONLY – APPROVAL TO REMOVE ENCRYPTION FROM DEVICE (DECRYPT)		
Chief or Deputy Chief Information Security Officer:	**Date:**	**Approved Denied** **Not Required**
RE-ENCRYPTION COMPLETION		
Re-encrypted by:	**Validated by:**	**Date:**

Chief or Deputy Chief Information Security Officer Signature

Signature:	Date:

Instructions for Certification of Temporary Export of UTEP Property and Review of U.S. Export Control Regulations Form

1. You should fill out the form and return to the Office of Compliance and Research Assurance (OCRA) prior to traveling abroad so that OCRA can determine whether an export license will be required for UTEP property being taken out of the country and verify that any foreign entities with which you will be working are not on any U.S. government restricted party list. **Please note - if you are taking potentially export-controlled items abroad, you should notify OCRA as early as possible, as obtaining an export license can take several months.**

2. **Destinations and Dates of Travel** - List all countries that you will be visiting while abroad. The requirements for an export license are based on the country of destination. List dates that you will be at each destination. If you are taking an item that is exempted under the Temporary Export License Exception (TMP), the item must be returned to the United States within one year.

3. **Purpose of the Travel** - Briefly describe the purpose of the travel (e.g. attending a conference, collaboration with university, conducting research, etc.).

4. **Contact with foreign individuals/entities** - You should list any specific foreign individuals, companies, or institutions that you plan to meet with while traveling abroad and provide a brief description of the purpose of the meeting. These entities will be screened so that you can be sure that they do not appear on any restricted party list issued by the U.S. government. While you will be provided with a list of restricted entities in the country you will be visiting, many restricted entities are not listed by country.

5. **Items removed** - You should list all electronic or scientific equipment owned by UTEP that you are taking abroad, whether tagged by inventory or not. This would include laptops, cellular telephones or other PDAs, GPS devices, sensors, or scanners, etc. Be as specific as possible in your description so that OCRA can make a determination on whether an export license would be required to take the item to the country of destination. For laptops, include any installed software other than the basic Microsoft Office Suite or similar commercially available applications. Be aware that the same regulations apply to any equipment you take that is your personal property. If you are taking a personal laptop, PDA, etc. you should review the regulations to ensure that those items do not require licenses as well.

6. **Authorization** – You must obtain authorization from your dean, director, or chair to remove equipment off campus. The Authorization form must be completed by your department.

7. **Classification of data** – Click the "Classification of Data on Device" tab listed above to classify your data. Based on the data classification you determine for your system; you are required to implement appropriate technical security measures to protect the data consistent with the university Minimum Security Standards. Confidential data has more stringent requirements than Controlled and Published classifications. All systems require some protective measures.