DoD Export-Controlled Technical Data (ECTD)
TECHNOLOGY CONTROL PLAN (TCP)

This plan covers the receipt, transfer, and/or use of DoD Export-Controlled Technical Data. All transfers of DoD export-controlled technical data must be conducted in accordance with U.S. Federal export-control regulations including but not limited to either the State Department's International Traffic in Arms Regulations (ITAR) at http://pmddtc.state.gov/regulations_laws/itar_official.html or the Department of Commerce's Export Administration Regulations (EAR) at http://www.access.gpo.gov/bis/ear/ear_data.html.

Export controlled technical information, data, materials, software, or hardware, (i.e., technology used in this project), must be secured from use and / or observation by unlicensed non-U.S. persons. In order to prevent unauthorized exportation of protected items / products, information, or technology deemed to be sensitive to national security or economic interests, a Technology Control Plan (TCP) is required.

In accordance with Export Control Regulations (EAR and ITAR), a Technology Control Plan (TCP) is required to prevent unauthorized export or transfer of controlled items, materials, information, or technology. This document serves as a basic template for the minimum elements of a TCP and the safeguard mechanisms that need to be put into place to protect authorized access or use. Security measures and safeguards shall be appropriate to the export classification involved. Assistance with this form is provided by the UTEP Export Control Officer (ECO) at exportcontrol@utep.edu.

Please indicate your specific access request as documented in the DD 2345:

Sponsor/Agency: _____

Proposal or Project ID: _____

Expected Start Date to receive DoD ECTD:

Technical Description of Export Controlled Material(s) to Be Received and/or Used:

PI: _____ **Dept:** _____

Phone: _____ **Email:** _____

PI Signature: _____ **Date:** _____

Co-PI:_____ **Dept:**_____

Phone:_____ **Email:**_____

Co-PI Signature: _____ **Date:** _____

Export Control Risks

When the sponsoring agency specifies information as ECTD and provides such information to the recipient, , the information has foreign national restrictions. In addition, the sponsor's approval must be obtained, consistent with the specified DoD Distribution Statement (A, C, D, or F), prior to publication or dissemination of research results that include ECTD. In such cases, UTEP will typically treat the use of ECTD as subject to U.S. export controls.

Transfers of DoD export-controlled technical data are subject to the requirements of the appropriate licensing department or agency. With respect to DoD export-controlled technical data covered under the U.S. Munitions List (USML), registration of the purchaser's, bidder's, transferee's business with the DoD may also be required. It is the responsibility of the purchaser, bidder, transferee to determine what the applicable requirements may be and to obtain all necessary authorization or approvals.

U.S. Federal export-controls cover all forms of transfer, including e-mails, faxes, and face-to-face conversations. Under U.S. law, providing controlled technology to a foreign person, whether within the U.S. or not, is deemed to be equivalent to physically exporting that technology to the country of the person's nationality.

Nondisclosure/Confidentiality: In most cases, proprietary information provided to UTEP under the DD 2345 Joint Certification Program will be presumed to be subject to U.S. export controls and may not be shared with foreign nationals without the approval of the Export Control Officer (ECO) and the sponsoring agency.

1. **Project Personnel:** All personnel who may have authorized access to the controlled technology\item must be identified (including their country of citizenship). The responsible person may request the addition or removal of project personnel at any time by submitting a revised TCP to the Export Control Officer (exportcontrol@utep.edu). Please use Appendix 1.

2. **Personnel Screening Procedures:** At a minimum, all persons that may have access to export-controlled materials or data must be listed on the TCP and screened against US government restricted persons/entities lists. Screening will be completed by the Export Compliance Office or their designee. For more information on the screening process please contact the Export Control Officer at exportcontrol@utep.edu.

3. **Physical Security Plan:** Project data and/or materials must be physically shielded from observation by unauthorized individuals.

   - **Location** (describe the physical location of the sensitive technology/item including building and room numbers: _____
     _____
     _____
     _____

   - **Physical Security:** (provide a description of your physical security plan designed to protect the item/technology from unauthorized access, i.e.., secure doors, limited access, security badges, locked desks or cabinets, secure computers, etc.):_____
     _____
     _____
     _____

- **Item Storage**: Both soft and hard copy data (i.e., notebooks, reports, and research materials) are stored in locked cabinets; preferably in rooms with key-controlled access. Describe how storage security will be ensured: _____

- **Markings:** Export-controlled items should be clearly marked with an appropriate warning, for example: *Warning – This contains export controlled technical data. Access or dissemination in violation of the ITAR and/or EAR may result in severe administrative (institutional) and criminal (individual) penalties.* When physical space is limited, an abbreviated warning may be used, for example *Export Controlled – Restricted.* Describe the markings or warnings that will be placed on export-controlled items and information or explain why they are not practical or possible. _____

Facilities Management has been contacted to provide assistance for the following:
(select all that apply)

☐ **Building/Room Access** ☐ **Solid Blinds** ☐ **Isolated Room request**

Other:

4. **Information Security Plan:** Please provide an outline of additional measures that will be taken to ensure information access controls including use of passwords and encryption protection for that data are applied to all controlled information. The data discard policy and relevant information technology policies and procedures should be included, as well as other plans for controlling access to controlled information. These procedures should address how computers on which controlled information will be stored. Any use of laptops for storage of export-controlled information must be justified and will only be approved with additional security measures.

   - *List all IT resources* (computers, servers, systems, etc.) that will be used to store or process export-controlled items and information: _____

   - IT security Plan (describe in detail your security plan, i.e., password access, firewall protection plans, encryption, etc.): _____

   - *Conversation Security* (Discussions about the DoD Export-Controlled Technical Data is limited to the approved and identified parties on the DD2345, and are held only in areas where unauthorized personnel are not present. Describe your plan for protecting export-controlled information in conversations: _____

- *Data storage and transmission*: External portable hard drives or flash drives, rather than shared central servers, are recommended for data storage provided physical storage is employed when they are not in use. Drives and devices used to store export-controlled items and information must be secured by encryption and password protection. For data storage on drives with network access or backup servers, the export-control items and information must be secured by encryption and password protection. Email may not be used for the transfer of export-controlled items or information subject to the ITAR or EAR. A secure file transfer method is preferred to transfer export-controlled items and information in electronic format.

    - Describe any project specific security methods or procedures that will be employed for data storage and transmission:_____

5. **Purchasing of Equipment:** Please provide the equipment that will or has been purchased through this award. Include the equipment name, description of equipment, vendor (name, email, and website), and ECCN or USML category if provided. All relevant purchasing documents are to be attached.

By printing and signing below, I, the Principal Investigator, agree to contact the Export Control Office prior to any change or proposed changes relating to project personnel, location, and/or security requirements.

Submitted by:_____ _____
Printed Name Date

Signature: _____

Export Control Officer Certification

○ Approved 'As Is' ○ Approved with Recommendation ◉ Denied

Screening Results Clear?	○ Yes	◉ No	Date:
Citizenship Requirements Verified?	○ Yes	◉ No	Date:
DD2345 Form Completed & Verified?	○ Yes	◉ No	Date:

Name: _____ Title: _____

Signed: _____ Date: _____

Comments: _____

_____

_____

Onsite audit and/or verification with Facilities Management on laboratory access:

Export Control Staff: **Date:**

Appendix 1 (Required)

Project Personnel: Clearly identify every person (including their country of citizenship) who may have authorized access to the controlled technology/item. Attach additional sheets if necessary. Please print.

	Name	Citizenship
1		
2		
3		
4		
5		
6		
7		

Appendix 2 (Required)

Training/Awareness Program: Mandatory Export Training: All participants listed on a TCP must receive mandatory export basic training prior to using any export-controlled items or technology. Contact the Export Control Officer if you require assistance at exportcontrol@utep.edu

	Participant Name	Date of Completion
1		
2		
3		
4		
5		
6		
7		

Appendix 3 (If Applicable)

Training/Awareness Program: CUI Training: All participants listed on a TCP that involves CUI must receive mandatory CUI training prior to receiving, transferring or handling CUI. Contact the Export Control Officer if you require assistance at exportcontrol@utep.edu. Attach additional sheets if necessary. Please type or print legibly.

	Participant Name	Date of Completion
1		
2		
3		
4		
5		
6		
7		

Appendix 4 (Required)

TECHNOLOGY CONTROL PLAN BRIEFING
(Must be signed by all persons with access)

This is to acknowledge that I have read and understand the UTEP Technology Control Plan. I have discussed the procedures with the sponsor/agency, and I agree to follow all of the procedures contained in the TCP. If I have any questions about this TCP, its requirements or following any procedure, I will contact the Export Control Office for advice before proceeding.

Signature:	Title:
Printed Name:	Date:
Signature:	Title:
Printed Name:	Date:
Signature:	Title:
Printed Name:	Date:
Signature:	Title:
Printed Name:	Date:
Signature:	Title:
Printed Name:	Date:
Signature:	Title
Printed Name:	Date:
Signature:	Title:
Printed Name:	Date:

Appendix 5 (Required)

CERTIFICATION FOR SAFEGUARDING EXPORT-CONTROLLED EQUIPMENT, MATERIALS, SOFTWARE, TECHNICAL DATA OR TECHNOLOGY

(Must be read and signed by all users prior to access of any export-controlled materials or data)

Sponsor/Agency Name: _____

Proposal or Project ID: _____

Researcher Name: _____

Statement: I understand that my participation on this Technology Control Plan will involve the receipt or use of export-controlled technology, items, software, or technical data, and that it is unlawful to transfer, send or take export-controlled materials or technology out of the United States. Furthermore, I understand that I may not disclose, orally or visually, or transfer by any means, export-controlled technology, or technical data to a non-U.S. person located inside or outside the U.S. without a license or applicable exemption as determined by UTEP's Export Control Officer.

A non-U.S. person is someone who is not a U.S. citizen or Lawfully Admitted Permanent Resident alien of the United States. **I understand the law makes no specific exceptions for non-US students, visitors, staff, postdocs, or any other person not pre-authorized under a TCP to access export-controlled materials or data**.

The export-controlled materials or technology of this project may not be exported to:

- Foreign countries and/or any foreign person, unless the University either obtains a license or determines that an exemption applies, and the University informs me of the same.
- Any and all embargoed destinations designated by the Office of Foreign Assets Control (located at http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx)
- Anyone found on the Specially Designated Nationals (SDN) list (located at http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)
- Proscribed countries or their citizens located in the United States as listed in 126.1 of the ITAR (if ITAR is applicable). http://pmddtc.state.gov/regulations_laws/documents/consolidated_itar/Part_126.pdf
- Any person or entity on the Denied Entity List, if EAR is applicable http://www.bis.doc.gov/entities/default.htm

For assistance with the restricted screening lists above, please contact the Export Control Officer at exportcontrol@utep.edu.

Reasonable Care. You may be held personally liable for violations of the export control regulations, (ITAR, EAR, OFAC). You must exercise care in using, sharing, and safeguarding export-controlled materials or technical data with others. Unless authorized by the appropriate government agency and notified to that effect by UTEP's Export Control Office, you may not export controlled materials or technical data to which you have been granted access.

If you foresee the need to export such information to a foreign country or foreign person (including, but not limited to, any University employees or students) as a part of your research at the University of Texas at El Paso, please inform the Export Control Office (exportcontrol@utep.edu) immediately to determine if an exemption is applicable or if a license or written assurance is needed.

You agree that you:

- Will not use or otherwise disclose the export-controlled materials for any other purpose other than what the agency/ sponsor has agreed upon.
- Will comply with any and all University of Texas at El Paso export control, security and access guidelines.
- Have been advised that technical data, computer software, materials or technology cannot be transferred to other non-U.S. persons without the prior written approval or other written authorization from the University of Texas at El Paso's Export Control Office who will determine if a license is required.
- Will not leave or place the export-controlled materials, software or technical information in any location or medium where there is risk that any unauthorized export may occur (including, but not limited to, placing export-controlled materials, unattended without effective safeguards, in non-password protected files, making export-controlled information accessible to the general public over the Internet, leaving any export controlled materials physically or visually accessible to non-authorized users, the campus community or public, and/or discussing attributes of the export-controlled materials or technical information where there is a risk of any unauthorized person overhearing).

Reminder: When using export controlled materials or technical data a license may be required for any type of physical export or release of technology, including but not limited to, communication with a non-U.S. person (such as face-to-face, telephone, email, fax, sharing of computer files, visual inspection, etc.), regardless of whether such non-US person is a student, faculty, visiting scholar/scientist, foreign collaborator, university staff, or member of the public.

Penalties: The penalties against individuals for unlawful export and disclosure of export-controlled information under the various export regulations can result in civil fines in excess of $1,000,000 and criminal penalties of up to $250,000 in fines and/or up to 10 years in prison.

Certification: I have read and understand the conditions of this certification and have received a copy of the Technology Control Plan as a part of UTEP's export control policy. I am electing to participate in the acceptance of DoD Export Controlled Technical Data within the Technology Control Plan and understand I could be held personally liable if I unlawfully disclose (regardless of form or format) export-controlled technology, technical data, materials, or software to unauthorized persons. I agree to address any questions I have regarding the designation, protection, or use of export-controlled information with the Export Control Office.

Please return this signed form to the Export Control Officer, Office of Research Compliance & Regulatory Assurances, or via email at exportcontrol@utep.edu.
Unsigned copies will not be accepted.

Participant Signature: _____Date: _____

Printed Name: _____ Title: _____