THESES\DISSERTATIONS
TECHNOLOGY CONTROL PLAN (TCP)

This activity involves or has the potential to involve the receipt and/or use of Export-Controlled Items or Information (ECII). As a result, the activity comes under the purview of 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) shall be required.

In accordance with Export Control Regulations (EAR and ITAR), a 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.

Establishing a TCP is a multi-step process requiring completion of a two-part form where: 1) the Student develops the TCP and submits it to the Chair; 2) once approved by the ECO, the Student is responsible for reviewing the control plan with all participants who individually sign off that the plan has been explained to them; 3) an individual certification form at the end of the TCP outlining the individual's responsibilities for handling export controlled materials or data is signed by each participant including the Student; 4) the Student submits a copy of all signed documents to the ECO, and keeps the originals with the project file, and implements TCP; 5) the Student notifies the ECO of any updates to the TCP as they occur (personnel, scope of work, safeguards, etc.).

Select the activity type:

- ◯ THESIS
- ◯ DISSERTATION

Title of Thesis\Dissertation: _____

NOA ID:
Cost Center ID:

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

Student:_____ **Department:** _____

Phone:_____ **Email:**_____

Chairperson:_____

Phone:_____ **Email:**_____

Student Signature: _____ **Date:** _____

Export Control Risks

Award Terms: When the terms of an award contain explicit export control requirements; foreign national restrictions; or require that the sponsor's approval be obtained prior to publication or dissemination of research results, UTEP will typically treat the project as subject to U.S. export controls.

Nondisclosure/Confidentiality: In most cases, proprietary information provided to UTEP under confidentiality conditions 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).

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 by defending in a space and during a time frame when observation by unauthorized persons is prevented.

   - **Location** (describe the physical location of the actual defense, 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 will be sanitized upon completion of the defense. 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 thesis\dissertation are limited to the identified committee members 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:_____

Statement: All listed participants understand that participation in the Thesis/Dissertation listed may 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 have briefed all listed participants that they 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.

I will ensure all participants:

- will not use or otherwise disclose the export-controlled materials for any other purpose other than this Thesis/Dissertation.
- 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).

By printing and signing below, I, the Committee Chair, agree to contact the Export Control Office prior to any change or proposed changes relating to the Thesis/Dissertation, 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:

Name: _____ Title: _____

Signed: _____ Date: _____

Comments: _____

_____

_____

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		