TECHNOLOGY CONTROL PLAN (TCP)

This project/activity involves or has the potential to involve the receipt and/or use of Export-Controlled Items or Information (ECII). As a result, the project/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 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.

Establishing a TCP is a multi-step process requiring completion of a two-part form where: 1) the PI develops the TCP and submits it to the ECO; 2) once approved, the PI 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 PI; 4) the PI submits a copy of all signed documents to the ECO, and keeps the originals with the project file, and implements TCP; 5) the PI notifies the ECO of any updates to the TCP as they occur (personnel, scope of work, safeguards, etc.).

Title of Sponsored Project/Activity: _____

Award ID:
Project ID:

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

Principal Investigator:_____ **Department:** _____

Phone:_____ **Email:**_____

PI 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.

   Screening Results Clear? **Yes** ◯ **No** ◯

3. **Physical Security Plan:** Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of "work-in-progress."

   - **Location** (describe the physical location of each sensitive technology/item including building and room numbers. A schematic of the immediate location recommended): _____

   - **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, notebooks, reports, and research materials are stored in locked cabinets; preferably in rooms with key-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing "export-controlled" technology are to be physically secured from unauthorized access. Describe how storage security will be ensured: _____

- **Markings:** Whenever possible 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. _____

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 system backup and who will have access, how computers on which controlled information will be stored will be sanitized upon completion of the project, and other procedures to provide necessary security. 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:_____

   - *List all individuals with administrative access* to IT resources who are **not** project personnel:_____

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

   - *Verification of technology/item authorization* (describe how you are going to manage security on export-controlled materials in the case of terminated employees, individuals working on projects, etc.): _____

   - *Conversation Security* (Discussions about the project or work product are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party subcontractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.) 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. *Note: Emailing export-controlled items or information subject to control regimes other than the EAR and ITAR will be considered on a case by-case basis but is* ***not*** *authorized unless specified below; when authorized to use mail, the sender is responsible for ensuring that the recipient is physically present in the U.S. at the time of transfer.*

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

Submitted by:_____ _____
Printed Name Date

Signature: _____

Information Security Office Certification

Approved 'As Is' ◯ Approved with Recommendation ◯ Denied ◯

Name: _____ Title: _____

Signed: _____ Date: _____

Comments: _____

_____

_____

Research Security Officer Certification

Approved 'As Is' ◯ Approved with Recommendation ◯ Denied ◯

Name: _____ Title: _____

Signed: _____ Date: _____

Comments: _____

_____

_____

Export Control Officer Certification

Approved 'As Is' ◯ Approved with Recommendation ◯ Denied ◯

Name: _____ Title: _____

Signed: _____ Date: _____

Comments: _____

_____

_____

Date of next TCP review is on (*TCPs will be reviewed on an annual basis***):**

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		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		

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		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		

Appendix 3 (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 for the stated project. I have discussed the procedures with the PI 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 PI for advice before proceeding. PI agrees to update this plan as required and as personnel are added to or deleted from this project.

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

Appendix 4 (Required)

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

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

Project Title: _____

PI Name: _____

Award ID: _____

Participant Name: _____

Sponsor: _____

Statement: I understand that my participation on the research project(s) 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 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 permanent resident alien (green card holder) 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 this research project.
- 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 research cited 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, Kelly Hall, Room 416, or via email at exportcontrol@utep.edu.
Unsigned copies will not be accepted.

Participant Signature: _____ Date: _____

Printed Name: _____ Title: _____