TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

OFFICE OF SPONSORED PROJECTS
TECHNOLOGY CONTROL PLAN (TCP) CERTIFICATION

PART I

Individual Requesting and Responsible for TCP:		
Telephone Number		
E-mail Address		
Request Date		
Description of Controls (EAR/ITAR Category)		
Location(s) Covered by TCP (add additional rows if needed)	Building Room(s)	
Project Personnel	List Name(s) below:	List citizenship(s) / Permanent Res. Status:
Personnel who will have access to export controlled subject matter (add additional rows if needed)		

Is research externally sponsored/funded?	Yes/No
If yes, identify sponsor:	
OSP Number and projected end date of project	

Is a non-disclosure agreement involved?		Yes/No
If yes, identify the parties:		
Contact Information:		
Attachments:		1. TCP 2. Export Briefing and Certification Form(s) for each person subject to this TCP
Approved:	_____ Vice President for Research or Designee	_____ Date

PART II
BRIEFING AND CERTIFICATION ON THE HANDLING OF EXPORT-CONTROLLED INFORMATION

This project involves the use of Export Controlled Technology and/or Information. As a result, the project may be subject to the export license requirements under the Department of State International Traffic in Arms Regulations (ITAR), or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.

It is unlawful under the ITAR and EAR to ship or take export controlled technology and/or information outside the U.S.; disclose, orally or visually, or transfer export controlled technology and/or information to a foreign national or entity inside or outside the U.S. without an export license or license exclusion or exception. A foreign national or entity is any individual who is not a U.S. citizen or permanent resident alien of the U.S, any foreign corporation or other entity or group that is not incorporated or legally organized to do business in the US and any foreign government. The law makes no exceptions for foreign graduate students who assist in research.

In general, research, activities, items, and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application utility may be subject to the export control regulations cited above. It does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of Export Controlled Technology and/or Information is military or civil in nature.

Researchers may be held personally liable for violations of the ITAR and EAR. During the course of your research, export controlled technology and/or information, must be secured from use and observation by unlicensed foreigners. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled Information up to and including jail.

Security measures will be appropriate to the classification involved. Examples of security measures include, but are not limited to:

- Project Personnel – Authorized personnel must be clearly identified.
- Laboratory "work in progress"- 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.
- Marking of Export-Controlled Technology and/or Information - Export-Controlled Technology and/or Information must be clearly identified and marked as export-controlled.
- Work Products - Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; preferably located in rooms with key-controlled access.
- Equipment or internal components – Tangible items and associated operating manuals and schematic diagrams containing identified "export-controlled" technology are to be physically secured from unauthorized access.
- Electronic communications and databases – Appropriate measures will be taken to secure export controlled electronic information. Such measures may include: User ID, password control, SSL or other approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using federally approved encryption technology.
- Conversations – Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the foreign national or entity limitations for such disclosures.

Department(s): _____

Research Project Title:

_____ OSP No. _____

Sponsor: _____

Certification: I hereby certify that I have read and understand this Briefing, and that I understand and agree to follow the procedures outlined above in the Technology Control Plan. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export controlled technology and/or information to unauthorized persons.

Signature: Date

_____

PART III

TECHNOLOGY CONTROL PLAN (TCP)

Research Project Title: _____

OSP No. _____ Date: _____

1) COMMITTMENT

Texas Tech University Health Sciences Center El Paso (TTUHSCEP) is committed to export controls compliance. The Office of Sponsored Projects (OSP) is responsible for implementation of technology control plans as applicable. The authorized official for export controls is the Vice President for Research. The Research Compliance Officer is the main contact for export control issues or questions. The individual responsible for and committed to ensuring compliance with this TCP is [Name of Responsible Party] _____.

2) BACKGROUND AND DESCRIPTION OF THE USE OF CONTROLLED ITEMS AND INFORMATION

_____

_____

_____

3) PHYSICAL SECURITY

[Description of how equipment, technology, data and other controlled information will be shielded from unauthorized persons including descriptions of relevant security systems such as badging, escorts, visitor logs and other types of building access restrictions.]

_____

_____

_____

4) INFORMATION SECURITY

TTUHSCEP Information Technology's (I.T.) guidance for protection and security of digital/electronic information found at http://www.ttuhsc.edu/IT/admin/policy/ will be followed for protection of controlled information under this TCP. All project data and other related digital materials will be strongly password-protected and encrypted using commercially available encryption technology. The computer(s) on which this data will be stored shall not be connected to any networks. When this computer has reached its usable life, the hard drive will be destroyed using university hard drive destruction services available through the IT Help Desk (http://www.ttuhsc.edu/IT/helpDesk)

[Outline additional measures that will be taken to ensure information access controls that will be utilized to ensure the requirements are met including use of passwords and encryption protection. 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, transmission procedures, how computers on which sensitive digital data will be stored will be sanitized upon completion of the project, and other procedures necessary to provide the necessary security. Use of laptops for storage of this data must be justified and will only be approved with additional security procedures.]

_____

_____

_____

_____

5) PERSONNEL SCREENING

All personnel with access to the export controlled technology and/or information and their nationality are listed in the TCP Certification Form. [List any information on the type of background check and any additional required reviews that will be employed beyond the University's standard background check procedures for all employees.]

_____

_____

_____

6) TRAINING AND AWARENESS

All personnel with access to export controlled technology and/or information on this project have read and understand the "Briefing and Certification on the Handling of Export-Controlled Information" for this project. Additional export control training for this project may be conducted by the OSP, Research Compliance Officer or others.

7) COMPLIANCE ASSESSMENT

Periodic evaluations and/or training to monitor compliance of the TCP procedures may be conducted during the course of this project. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP must be approved in advance by the Vice President for Research.

8) PROJECT TERMINATION

Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminated when the information has been destroyed or determined to be no longer export-controlled.