

Technology Control Plan (TCP)

Instructions: Fill out the Project Information section and describe the export prevention procedures in response to Questions 1 – 6. Some fields contain example language. Use the example language to guide the creation of your plan and remove unnecessary example language as needed. Submit the completed TCP to ResearchCompliance@smu.edu for review and signatures.

2. Describe how the locations containing export-controlled items, technology, and software will be protected from unauthorized access. Describe how access will be revoked if necessary.

Information Security Plan

3. Describe how controlled technology and software will be secured from unauthorized access. Include methods of data transfer, if applicable. Describe how access will be revoked if necessary. Describe the plan for protecting controlled information during conversations and informal discussions. Include provisions for preventing exports during international travel. Include provisions for destruction or disposal of technology and software at conclusion of project.

Item Security Plan

4. Describe how tangible items will be clearly identified and secured from unauthorized access. Include provisions for preventing exports during international travel. Include provisions for destruction or disposal of tangible items at conclusion of project.

Project Personnel

5. Identify all persons who will have access to the controlled items, technology, and software. Include contractors, if applicable.

<u>Name</u>	<u>SMU ID</u>	<u>Date of Birth</u>	<u>Project Role</u>	<u>Country of Citizenship</u>
			Principal Investigator	

Training and Education Program

6. Describe how project personnel will be educated in export controls regulations and the procedures described in this document. Also describe how laboratory personnel who are not included in this project will be educated regarding the procedures described in this document.

Research Compliance and OIT Confirmation

- ☐ All project personnel have passed public records check and screening on the Consolidated Screening List
- ☐ All project personnel have completed CITI Export Controls training
- ☐ Information security measures are sufficient
- ☐ Physical security measures are sufficient

Director of Research Compliance

Chief Security Officer

SMU Police Department

Mary Travis

Corinna Taylor

Chief Jim Walters

Certification and Signatures

As a designated Project Personnel on this Technology Control Plan, you may have access to Export-Controlled items, technology, and/or software subject to International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).

Reasonable Care: You may be held personally liable for violations of the ITAR or EAR. As a result, you should exercise care in using and sharing Export-Controlled items, technology, and software with others. Export-Controlled items, technology, and software must be handled in accordance to the security plans and/or controls specified in the Technology Control Plan and only shared with authorized Project Personnel. In the absence of that clearance, PIs should not leave Export-Controlled items, technology, and software unattended.

Penalties: Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled items, technology, and software up to and including incarceration. All fines and penalties are cumulative.

Certification: I certify I have read, understood, and will adhere to this Technology Control Plan and applicable EAR and ITAR regulations.

<u>Name</u>	<u>Signature</u>	<u>Name</u>	<u>Signature</u>