Technology Control Plan (TCP)

Part 1

Faculty/Staff responsible	
Applicable time period	

Name of controlled items, Type of control and classification, & Provider of controlled items (where applicable)	

Location & Security

List of PERSONNEL having access to the controlled item

Full Legal Name	Citizenship & status	Affiliation

Prior to accessing the controlled material/activity, all personnel must:

- **sign the TCP certification form and send it to the Export Controls Official;**
- **be screened and approved by the Export Controls Official.**

Certification: I hereby certify that all personnel have been provided with a copy of the TCP and have been informed of their obligations under the TCP. I understand that I could be held personally liable for civil and/or criminal charges if I unlawfully disclose, regardless of form or format, Export-Controlled item, technical data or software to unauthorized persons.

_____

Printed name and title of Requestor

_____

Requestor Signature & Date

For Use by the Export Controls team			
Request:	Approved	Denied	
Comments:			
RPS completed on:		**No Red Flag**	Red Flag
Comments:			

Allen A. DiPalma, Director-Office of Trade Compliance

Printed name and title

_____

Export Controls Official Signature & Date

Part 2

This project involves the use of U.S. Export-Controlled information, equipment, or software. As a result, the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), or other U.S. Export-Control regulations apply to the project.

In general, "Export-Controlled" means that activities, items, information, technology, and software related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, processing, or use of a controlled item requires an export license, or license exception, to physically export from the U.S. OR to discuss with or disclose to a person who is not a U.S. citizen or lawful permanent U.S. resident.

Basic marketing information on function or purpose; general system descriptions; information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities; published information in the public domain; and published patent information is **not** Export-Controlled. Information developed as a result of fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published, without any publication restriction or publication approval requirement is **not** Export-Controlled.

It is unlawful to send or take Export-Controlled information, technology, software, or items out of the U.S.; or disclose, orally or visually (including by email, fax, phone, etc.), or transfer to a foreign person inside or outside the U.S. without prior authorization from the cognizant U.S. government agency. A foreign person is a person who is not a U.S. citizen or lawful permanent resident alien of the U.S. A person lawfully in the U.S. on a visa for work or study is a foreign person. The law makes no exceptions for foreign graduate students or visiting scientists.

Researchers may be held personally liable for civil or criminal violations of the U.S. Export-Control Regulations. As a result, you should be clear on the requirements and exercise reasonable care in using and sharing Export-Controlled information, technology, software, or items with others. This Technology Control Plan is to help you assess, address, understand your obligations, and control access to the Export-Controlled aspects of this project.

The security measures designed and implemented should be appropriate to the type, nature, and level of Export-Controlled information, technology, software, and/or items involved in the project. Examples of appropriate security measures include (but not limited to):

• Project Personnel - Authorized personnel must be clearly identified in part 1. Ensure changes to this list are provided prospectively to the Export Control officer.

• Laboratory "work-in-progress" – Plans to protect project data and materials from observation or access by unauthorized individuals. This would include operating in secured laboratory spaces or during secure time blocks when observation by unauthorized persons is prevented.

• Marking of Export-Controlled Information - Export-Controlled information must be clearly identified and marked as export controlled with a legend appropriate to the applicable control.

• Equipment, components, or other Items or technical data – Equipment, parts, components, or other items (including technical data) and associated operating manuals, diagrams, etc. containing identified export-controlled information or technology are to be physically secured from unauthorized access.

• 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 address the non-U.S. citizen limitations for such disclosures.

• Phones, PDA's, Tablets, Computers, MP3 Players, and Other Personal Electronics – No export-controlled data or information should be loaded to, sent to, or stored on any personal electronic device.

Certification: I hereby certify that I have read and understand this Briefing, and that I understand and agree to follow the procedures outlined in the TCP. I understand that I could be held personally liable for civil and/or criminal charges if I unlawfully disclose, regardless of form or format, Export-Controlled information, technology, software, or items to unauthorized persons.

Signature: _____

Printed Name:_____

Date: