The University of Pittsburgh - Office of Export Controls Services (OEC)
Technology Control Plan (TCP) Certification for Export Controlled Item

Part I- TO BE COMPLETED BY REQUESTING UPITT FACULTY MEMBER

Name of Upitt faculty member who is Requesting and Responsible for TCP (Requestor):	
Telephone Number:	
E-mail Address:	
Department:	

Description of Controlled Item	
Location(s) of controlled item Covered by TCP (add additional rows if needed)	Building name and room #:

Project Personnel*	List **FULL LEGAL** Name(s) below:	List citizenship(s) / Permanent Res. Status:
List ALL Personnel who will have access to export controlled item (add additional rows if needed)	First, Middle, Last (no nicknames) Name 1 Name 2 Name 3	 Country and Status: Country and Status: Country and Status:

Is the export controlled item to be used in externally sponsored research? *	Yes ☐ No ☐
If yes, identify each sponsor and the title of project (add additional rows if needed)	
Provide OR Info Ed Institution Number or I#	
Projected start date and end date of project	Start Date: End Date:

Is a UPitt non-disclosure agreement (NDA or CDA) associated with use of the export controlled item?	Yes ☐ No ☐ +If yes, please attach copy
If yes, identify the parties to the NDA/CDA:	
Provide OR Info Ed Institution Number or I#	

REQUESTOR COMMENTS (optional):

Attachments	Please attach these items to this request	1. Export Briefing and Certification Form(s) for each person named in personnel 2. Technology Control Plan 3. NDA/CDA if any
Requestor	Signature: Note that no digital or "per" signatures are permitted.	Date
Chair or Director	Signature: Note that no digital or "per" signatures are permitted.	Date

FOR OR USE ONLY Upitt Authorized Official Approval O. Export Controls 412-624-7415	_____ Allen A. DiPalma, Export Controls Officer & Empowered Official Date

*NOTE: Any changes to personnel named or scope of use of controlled item requires the prospective review and approval of the University Export Control Officer.

Part II: Briefing and Certification on the Handling of Export-Controlled Information

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.
- Work Products – Paper data, lab notebooks, reports, and research materials are stored in locked cabinets, preferably located in rooms with key-controlled access.
- Equipment, components, or other Items – Equipment, parts, components, or other tangible items 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: _____ Note that no digital or "per" signatures are permitted. Printed Name:_____	Date:

CERTIFICATION INSTRUCTIONS:

PRINT AND EXECUTE THIS **CERTIFICATION** FORM FOR EACH PERSON NAMED IN PART 1 WHO WILL HAVE ACCESS TO EXPORT CONTROLLED ITEM.

Part III: Technology Control Plan (TCP)

1 Commitment

The University Pittsburgh is committed to export controls compliance. The Office of Export Controls Services is responsible for institutional oversight of technology control plans as applicable. The Export Control Officer and Empowered Official is Allen A. DiPalma. The Export Controls Officer is the main contact for export control issues.

The Upitt faculty member responsible for and committed to ensuring compliance with this TCP is:

2 Background and Description of the Use of Controlled Items and Information

Please provide a brief overview of the project that will utilize export controlled item. Describe what sensitive data and materials will be utilized and to whom and how they will be delivered.

3 Physical Security

Please describe the physical security controls that will be used to prevent unauthorized access to secured areas and to protect project materials and computers. At a minimum, these controls should cover the bullet point items in Part II above and the following:

- Plans to ensure that work for this project is done only within secured areas.
- Plans to protect materials (physical or digital) and to ensure that project materials not leave the secured areas (including via the network).
- Plans for clearly marking all physical materials (e.g. hardcopy, removable media, etc.) as export-controlled, propriety, and/or subject to an NDA as appropriate. The plan should provide that materials be physically secured from access when not in use.
- Procedures to ensure that only approved project members listed on this TCP who have signed certifications are present in the secured areas when work on this project is being performed.
- Plans to prevent non-U.S. persons viewing or having access to any project data (physical or digital) or secured area (including maintenance, cleaning, and others).

4 Information Security

The University of Pittsburgh will require that all researchers subject to a TCP ensure that sensitive digital research data is appropriately protected.

Please explain, in sufficient detail, what information security controls will be used to protect sensitive project data. At a minimum, your plan must comply with the bullet point items in Part II above and the following guidelines:

- Any requirements explicitly outlined in the contract/NDA, such as technology controls, data classification, encryption, network access (or lack thereof), non-disclosure, secure destruction, etc., must be adhered to at all times.
- Project data must not be sent unencrypted over any networks. All data stored on computers and removable media must be encrypted at rest, utilizing a whole disk encryption product wherever feasible.
- Project computers must be dedicated exclusively for work that is covered by a Technology Control Plan, and not be general-purpose machines.
- Project computers should not be Internet accessible unless explicitly allowed by the data owner. If project computers are to be Internet accessible, operating system and application patches must be applied in a timely manner. If applications provide an automatic update feature, it should be utilized.
- Project computers should be non-networked unless network connectivity is required for project work. If network connectivity is required, project computers should be configured to deny all non-essential inbound and outbound traffic. Network connectivity must be restricted to the maximum extent feasible. MAC addresses for all Ethernet and wireless interfaces must be provided to the Information Security Office.

5 Personnel Screening

Only approved project members listed on this TCP who have signed certifications shall be permitted access to controlled item.

6 Training and Awareness

All approved project members with access to export-controlled items on this project have read and understand the information contained in this packet. Additional export control training for this project may be conducted by the Export Controls Officer. The Office of Export Controls Services also provides periodic training sessions to members of the Pitt community.

7 Compliance Assessment

As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed by the Requestor and any findings reported to the Export Controls Officer at

dipalma@pitt.edu (412-624-7415). The Export Controls Officer may also conduct periodic audits and/or training to monitor compliance of the TCP procedures.

Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be reviewed and approved in advance by the Export Controls Officer.

8 Project Termination

Security measures will be required for export controlled items after the project termination. Please describe the security measures to remain in effect for export controlled items following termination of the project: