Carnegie Mellon University
Office of Research Integrity and Compliance

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 Export Compliance Office at export-compliance@andrew.cmu.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: _____

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

Principal Investigator: _____ **Department:** _____

Phone: _____ **Email:** _____

Pre-determined Export Classification: ECCN: _____ **(e.g. 5D002) <OR> ITAR Category:** _____ **(e.g., VII (e))**

If you do not have the ECCN or ITAR Category, contact your sponsor or program manager for this vital information. This form cannot be processed without the applicable EAR ECCN or the ITAR Category.

PI Signature: _____ **Date:** _____

1. **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: _____

   Name & Citizenship: _____

   Name & Citizenship: _____

   Name & Citizenship: _____

   Name & Citizenship: _____

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 Compliance Officer at export-compliance@andrew.cmu.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** (include building and room numbers, lab name, etc.): _____
   - **Physical Security:** Provide a description of your physical security plan designed to protect the item/technology from unauthorized access, (e.g., 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: _____

     _____
   - **Destruction or Return of Materials**: Describe how the export controlled will be handled at the end of the project or when they are not needed anymore, (shredding, file wipes, destroy hard drive, return to sponsor, etc.). _____

     _____

4. **Information Security Plan:** Appropriate measures must taken to secure controlled electronic information, including User ID's, password control, SSL etc. Example: database access shall be managed via a Virtual Private Network (VPN), allowing only authorized persons to access and transmit data over the internet, using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology. Describe what information security safeguards will be used**:** _____

   _____

5. **Training/Awareness Program - Mandatory Export Training**: All participants listed on a TCP must receive mandatory export basic training by the Export Compliance Office prior to using any export controlled items or technology. Contact the Export Compliance Office to schedule a project training session at export-compliance@andrew.cmu.edu.

Date Training Scheduled: _____ **Date Export Training Completed:** _____

Participant: _____

Participant: _____

Participant: _____

Participant: _____

Participant: _____

TECHNOLOGY CONTROL PLAN BRIEFING
(Must be signed by all persons with access)

This is to acknowledge that I have read and understand the Carnegie Mellon University Technology Control Plan for the stated project. I have discussed the procedures with the PI and I agree to the 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: _____

Approved by Signature: _____ Date: _____

Title: _____

Carnegie Mellon University
Office of Research Integrity and Compliance

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: _____

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 CMU's Export Compliance 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 Compliance Office at export-compliance@andrew.cmu.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 Carnegie Mellon's Export Compliance 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 Carnegie Mellon, please inform the Export Compliance Office (export-compliance@andrew.cmu.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 the research referenced below;
- will comply with any and all Carnegie Mellon University export control, security and access guidelines;
- have been advised by Carnegie Mellon herein that the technical data, computer software, materials or technology cannot be transferred to other non-US persons without the prior written approval or other written authorization from Carnegie Mellon 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-US 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 Carnegie Mellon University's export control policy. I am electing to participate in the research cited above, 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 Compliance Office.

Please return this signed form to the Export Compliance Office, Office of Research Integrity and Compliance (ORIC), WQED Building, 2nd Floor, or via email at export-compliance@andrew.cmu.edu. **Unsigned copies will not be accepted**.

Participant Signature: _____ Date: _____

Printed Name: _____ Title: _____