UNIVERSITY OF NOTRE DAME | OFFICE OF THE VICE PRESIDENT FOR RESEARCH

Technology Control Plan (TCP)

This project involves or has the potential to involve the receipt and/or use of Export-Controlled Items or Information (ECII). As a result, the project comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR) or the Department of Commerce's Export Administration Regulations (EAR). Links to information about EAR and ITAR regulations can be found on Notre Dame's Research Compliance Website.

It is unlawful under the EAR or ITAR to send or take Export-Controlled items or information out of the U.S. This includes disclosing information orally or visually, or transferring export-controlled items or information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, an export license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

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 Office of Research Compliance at (574)631-1389 or compliance@nd.edu.

Establishing a TCP is a multi-step process and two-part form where: **1)** the PI develops the TCP and submits it to the Office of Research Compliance; **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 Office of Research Compliance, 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).

Date:

Title of Sponsored Project/Activity:

Technical Description of Export Controlled Material(s) to be received and/or Used:

Principal Investigator:

Department:

Department Address:

Phone:

Email:

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 the Office of Research Compliance for this vital information.

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:** ______________________________
   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. The Office of Research Compliance will complete screening.

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").

   a. **Location** (describe the physical location of each sensitive technology / item to include building and room numbers. Attachment of a diagram of the location is highly recommended):

   ____
   ____
   ____
   ____
   ____

   b. **Physical Security** (provide a detailed description of your physical security plan designed to protect your item/technology form unauthorized access, i.e., secure doors, limited access, security badges, CCTV, etc.):

   ____
   ____
   ____
   ____
   ____

   c. **Perimeter Security Provisions** (describe perimeter security features of the location of the protected technology / item):

   ____
   ____
   ____
   ____
   ____

4. **Information Security Plan** (Appropriate measures must taken to secure controlled electronic information, including User ID's, password control, SSL or other approved encryption technology. Database access must 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).

    a. **Structure of IT security** (describe the information technology (IT) setup / system at each technology / item location:

    b. **IT Security Plan** (describe in detail your security plan, i.e., password access, firewall protection plans, encryption, etc.):

    c. **Verification of Technology/Item Authorization** (describe how you are going to manage security on export controlled materials in the case of terminated employees, individuals working on new projects, etc.):

    d. **Conversation Security** (Discussions about the project or work product are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party subcontractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures. Describe your plan for protecting export controlled information in conversations):

5. **Item Security**

    a. **Item Marking** (Export controlled information must be clearly identified and marked as such):

    b. **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):

6. **Training / Awareness Program** (The University of Notre Dame requires export control training via an institutional subscription to the Collaborative Institutional Training Initiative (CITI), a consortium of universities that provides convenient and comprehensive online training modules, for all faculty, graduate students, and post-doctoral students who anticipate working in export controlled areas or anticipate submitting an export control license (or exception). Certification is good for five years, and it must be complete before beginning work.

All participants listed on a TCP must receive mandatory export basic training.

Participant: ______________________ **Date Export Training Completed:** __________
Participant: ______________________ **Date Export Training Completed:** __________
Participant: ______________________ **Date Export Training Completed:** __________
Participant: ______________________ **Date Export Training Completed:** __________
Participant: ______________________ **Date Export Training Completed:** __________
Participant: ______________________ **Date Export Training Completed:** __________

7. **Self Evaluation Program**

   a. **Self Evaluation Schedule** (describe how often you plan to review / evaluate your TCP):

   b. **Audit Checklist** (provide a checklist for items reviewed during self evaluation audits):

   c. **Action Item and Corrective Procedures** (describe your process to address findings in your self evaluation audits):

Technology Control Plan Briefing
(Must be signed by all with access)

This is to acknowledge that I have read and understand the University of Notre Dame 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 of 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:** ________________________

Signature: ______________________________ **Title:** ________________________
Printed Name: ______________________________ **Date:** ________________________

Chair Signature: ______________________________ **Date:** ________________________

Vice President for
Research Signature: ______________________________ **Date:** ________________________

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 Office of Research Compliance, (574)631-1389 or compliance@nd.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 Officer, 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 the University of Notre Dame, please inform the Office of Research Compliance 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 University of Notre Dame export control, security and access guidelines;

- have been advised by Notre Dame 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 Notre Dame 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 University of Notre Dame'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 Office of Research Compliance. Please return this signed form to the Office of Research Compliance, 317 Main Bldg. Unsigned copies will not be accepted.

Participant Signature: ______________________________ **Date:** ______________________________

Printed Name: ______________________________ **Title:** ______________________________