**Technology Control Plan (TCP)**

***Background.*** This project/activity involves or has the potential to involve the receipt and use of Export-Controlled Information. 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) <http://www.access.gpo.gov/bis/ear/ear_data.html>.

It is unlawful under the EAR or ITAR to send (in any way) or take Controlled Objects (defined below) out of the U.S. or disclose (in any way) any Controlled Object to any foreign person in the U.S., without, in either case, a license or an applicable license exception. A foreign person **means both (i) any foreign entity or group not incorporated or organized to do business in the U.S., and/or (ii) any person who is not a (a) U.S. citizen, (b) permanent resident of the U.S. (i.e., a “green card” holder) or (c) political asylee or refugee status holder.** 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 Objects**.**

Controlled Objects, including, for example, technical information, data, materials, software, or hardware, (i.e. technology used in this project or activity), 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) is required.

In accordance with Export Control Regulations (EAR and ITAR), a TCP is required to prevent unauthorized exportation of controlled materials, items, technology, equipment and information determined to be subject to export control requirements. Given this determination, the University is required to limit access to and use of these materials, items, technology, equipment and information (collectively referred to as Controlled Objects).

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, use or disclosure of Controlled Objects. Security measures and safeguards shall be appropriate to the export classification involved. A variety of factors must be taken into account to determine who may have access to Controlled Objects; for this reason, only the individuals identified below may have access to and use of such Controlled Objects to the extent stated in this TCP.

***Establishing a TCP.*** (A) As a general matter, the identification of any object as having either an Export Control Classification Number (ECCN) or classification on the United States Munitions List (USML) triggers, among other things, the need for a TCP to be completed, monitored and revised as appropriate.

(B) For purposes of this form, the term “PI” means the Primary Investigator at the University having overall responsibility for the research project or activity. The term “RI” means the individual at the University having overall responsibility for the non-research project or activity.

(C) Establishing a TCP is a multi-step process and two-part form as follows:

**1)** the PI or RI (defined below) develops and prepares the TCP with, as explained below, the assistance of the ITS department (and such other departments as necessary) and obtains all necessary departmental or college level signatures;

**2)** the PI or RI is responsible for reviewing the approved TCP with all participants and obtaining from each participant a signed copy of thethe **Certification for Safeguarding Export Controlled Objects (**including the PI or RI);

**3)** the PI or RI submits a copy of all signed documents, including the certifications to the appropriate department and keeps the original documents with the project/activity file on file with his or her department;

4) the PI or RI implements and monitors compliance with the TCP; and

**5)** the PI notifies Associate Vice Provost for Research Compliance or the University Compliance Officer, as appropriate, of all updates to the TCP as they occur (personnel, scope of work, safeguards, etc).

(D) Completed TCPs relating to research Controlled Objects are submitted to the Office of Research Administration (ORAF). Completed TCPs relating to non-research Controlled Objects are submitted to the University Compliance Department. Guidance with respect to completing this form is provided by ORAF and/or the University Compliance Department, as applicable. Notwithstanding the filing of the TCP in the applicable office, as stated throughout this TCP, the PI or RI bears primary responsibility for compliance with the TCP and applicable regulations.

(E) The PI or RI signing the TCP must retain copy of the completed TCP (and all subsequent changes thereto) in his or her department’s files and, as stated above, timely provide one copy (including all subsequent changes) to either ORAF and/or the University Compliance Department, as appropriate.

***Protecting the TCP Itself.*** Only the PI or RI, the participants on the project or activity and the necessary University employees in either ORAF or the Compliance Department (and such other University departments as may, from time to time be necessary) shall receive, complete, review and/or revise this TCP. **Given the sensitive nature of a completed form of TCP, the PI or RI, as applicable, shall ensure that all draft, final and subsequent versions of this TCP are transmitted and maintained in a manner that safeguards the contents of this TCP from unauthorized access, use and disclosure.** Therefore, for example, the PI or RI shall not transmit electronically any version of a completed or partially completed TCP without taking appropriate steps to protect the contents of the TCP from unauthorized access, use and disclosure.

**Background Information:**

|  |  |  |
| --- | --- | --- |
|  | **Date:** |  |

|  |  |  |
| --- | --- | --- |
|  | **Title and full description of the Project or Activity (including start and end dates)** |  |

The following description should clearly identify the Controlled Objects that will be protected under this TCP and include the type of Controlled Object (for example, Materials (synthetic or natural), Hardware (Item/Equipment), Software, Information (hard copy and/or electronic copy)), whether the Controlled Object is Controlled by ITAR, EAR or other regulations, and, as applicable, the USML list category and subparagraph, Export Control Classification Number (ECCN) if subject to the EAR or other agency regulations (e.g., Department of Energy nuclear regulations).

|  |  |  |
| --- | --- | --- |
|  | **Technical Description of Materials Item/Technology/Equipment/Software to be used in the Project or Activity:** |  |

|  |  |
| --- | --- |
| **Contract, Grant or other Document Reference to which this TCP Applies (Include Names of Parties, Date, any project award number and general description of the relevant Agreement and attach a copy of the Agreement to this TCP):** |  |

|  |  |  |
| --- | --- | --- |
|  | **Responsible Individual (Project Manager / Principal Investigator {PI}) and Department:** |  |

|  |  |  |
| --- | --- | --- |
|  | **Campus Address:** |  |

|  |  |  |
| --- | --- | --- |
|  | **Phone:** |  |

|  |  |  |
| --- | --- | --- |
|  | **E-mail:** |  |

1. **Physical Security Plan: All Controlled Objects, including technology, requiring a license under ITAR, EAR or OFAC regulations must be physically protected against export and deemed export without applicable license.** All Controlled Objects including without limitation technology, project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory and/or other spaces, or during secure time blocks when observation by unauthorized persons is prevented. Project or activity personnel within the restricted area must be responsible for challenging all persons who may lack appropriate access authority.
   1. **Location**. Locations where the project or activity is to be performed with Controlled Objects must have restricted access. Restricted access generally means having a clearly defined perimeter that adequately protects against oral, in the case of discussions concerning the Controlled Object, and visual disclosure of the Controlled Objects. Electronic devices containing Controlled Objects must be physically secured or in the possession of a member of the project or activity at all times. The security of electronic files should be addressed in the Information Security section below. Describe the physical location of each Controlled Object to include building and room numbers. Attachment of a diagram of the location is highly recommended:

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Physical Security** Provide a detailed description of your physical security plan designed to protect your Controlled Objects from unauthorized access, ie., locked storage, secure doors, limited access, security badges, CCTV, etc.:

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Perimeter Security Provisions** Describe perimeter security features of the location of the Controlled Object:

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Information Security Plan for Controlled Object** Appropriate controls must taken to secure all Controlled Objects, including electronic Controlled Objects. Controls may include User ID’s, password control, SSL and other University 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. In addition, computers used to access or store Controlled Objects must run on University-approved operating systems with the latest security service packs and patches.
   1. **Structure of IT security** Describe the information technology (IT) setup / system at each location where the Controlled Object is present:

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **IT Security Plan** Only authorized project or activity personnel should be designated users of computers and servers used to access or store Controlled Objects on those computers and servers. At a minimum, a valid account and password must be provided to gain access to Controlled Objects on such computers and servers. Only project or activity personnel may retain this login information and no other login accounts may be created. Both failed and successful logins must be logged internally. Firewalls must be installed on all computers to secure and monitor network access to/from the computer containing the Controlled Object. If the firewall in disabled to allow proper data collection, wired and wireless internet connections must be disabled. Describe in detail your security plan, i.e., password access, firewall protection plans, encryption and other specific security measures, devices or procedures that will be used to protect the Controlled Object from unauthorized access, use or disclosure.

|  |  |  |
| --- | --- | --- |
|  |  |  |

Data Storage and Transmission. External portable hard drives or flash drives, rather than shared central servers, are recommended for data storage provided physical storage is employed when they are not in use. Drives and devices used to store Controlled Objectsmust be password protected or encrypted. For data storage on drives with network access or backup servers, the Controlled Objectmust be secured by encryption and password protection. Email may not be used for the transfer of Controlled Objectssubject to the ITAR or EAR. A secure file transfer method (SSH/SCP/SFTP/SSL) or mailing a disk or flash drive are preferred methods to transfer Controlled Objectsin electronic format. *Note: Emailing Controlled Objects subject to control regimes other than the EAR and ITAR will be considered on a case-by-case basis, but is not authorized unless specified below; when authorized to use email, the sender's is responsible for ensuring that the recipient is physically present in the US at the time of transfer.* Describe any project or specific security methods or procedures that will be employed for data storage and transmission of Controlled Objects.

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Verification of Permissions to Controlled Object** Describe how you are going to manage security on Controlled Objects in the case of terminated employees, individuals working on new projects, etc:

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Conversation Security** Discussions about the project or activity and Controlled Objects are limited to authorized project or activity personnel 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 Controlled Objects in conversations:

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Cloud Computing** Unless specified below, no cloud or similar computing facilities or services will be used to store, process or transfer Controlled Objects. Describe any intended used of cloud or similar computing facilities or services used in connection with the Controlled Objects.

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Controlled Object Security**
   1. **Controlled Object Marking** Whenever possible, Controlled Objects must be clearly marked with an appropriate warning (given any space limitations) such as *WARNING – This contains [ITAR] controlled technical data. Access or dissemination in violation of the ITAR may result in several administrative (university) and criminal (individual) penalties. Contact the University Compliance Department if you find this item/document unsecured*. Describe the markings or warnings that will be placed on the Controlled Objects or explain why they are not practical or possible:

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Controlled Object Storage** Both soft and hard copy data, notebooks, reports and all other items, technology, data materials and other Controlled Objects information 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:

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Project/Activity Personnel** All participants listed on a TCP must receive mandatory export control basic training.All such participants needing or having access to a Controlled Object must be clearly identified below and sign the form of **Certification for Safeguarding Export-Controlled Objects** attached to this TCP prior to accessing or participating in the project or activity. The PI or RI, as applicable may request the addition or removal of project or activity personnel at any time by completing and submitting a revised TCP to the University Compliance Department. Clearly identify every person (including their national citizenship) who is determined to have authorized access to the Controlled Object item and will be working on this project/activity. Attach additional sheets if necessary. Please print. For each person, state the date the person successfully completed the University tutorial on Export Controls. Such person must complete the tutorial prior to having access to Controlled Objects or participating in this project or activity.

|  |  |  |
| --- | --- | --- |
|  | **Name/ Title/Citizenship/ Date EC Training Completed:** |  |
|  | **Name/Title/ Citizenship/ Date EC Training Completed:** |  |
|  | **Name/Title/ Citizenship/ Date EC Training Completed:** |  |
|  | **Name/Title/ Citizenship/ Date EC Training Completed:** |  |
|  | **Name/ Title/**  **Citizenship/ Date EC Training Completed:** |  |

1. **Personnel Screening Procedures** 
   1. At a minimum, the PI or RI identified above must ensure all project or activity personnel are screened against the applicable list of restricted and denied parties lists published by the government. Contact the ORAF or University Compliance Department, as appropriate for assistance performing that review. The PI or RI identified above shall not allow project or activity personnel access, use or disclosure of Controlled Objects until the individual has signed attached **Certification for Safeguarding Export-Controlled Objects** and completed the required tutorial and screening.
   2. **Background Checks** (describe types of background checks performed on persons with access to controlled technologies / items, e.g., criminal, drivers license, etc.):

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **Third Party Contractors** (if any will use the controlled item, technology, data, materials and other information, describe security screening procedures for temporary employment agencies, contractors, etc.):

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Training / Awareness Program** 
   1. **Foreign Nationals** (Describe schedules and training for informing foreign national employees involved in the project/activity technology access limits; if no such persons will be involved on the project, state no such persons will be involved on this project):

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. **U.S. Employees** (describe schedules and training for informing employees who are U.S. citizens and involved in the project with project/activity technology access limits.

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Self Evaluation Program** Relevant findings should be reported to the Compliance Officer promptly.
   1. **Self Evaluation Schedule** (Describe how often you plan to review / evaluate this TCP. Annual reviews are highly recommended):

|  |  |  |
| --- | --- | --- |
|  |  |  |

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

|  |  |  |
| --- | --- | --- |
|  |  |  |

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

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **International Travel** (Describe any international travel associated with this project or activity. If there will be any such travel, fully identify the persons who will travel, to where, the purpose of the trip and its duration. If none, so indicate.)

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Project Specific Export Authorizations Required**. Specify any intended exports of Controlled Objectsin the section below. Inclusion in this section does NOT, in and of itself, constitute approval to export; it is rather an indication to Export Control Committee that an export license or other authorization may be needed. This prohibition on exports includes, but is not limited to, exports to foreign nationals in the U.S., as well as the permanent or temporary shipment or transfer of Controlled Objectsout of the US.

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Recordkeeping** US export control regulations require retention of records associated with all exports, use of license exceptions and certain other activities. The PI or Responsible Party identified above or Department shall be responsible for keeping records for the required five years from the date of the last related activity or longer if necessary to comply with regulatory requirements or the terms and conditions of any applicable award. Specify all planned exports of Controlled Objects.

|  |  |  |
| --- | --- | --- |
|  |  |  |

1. **Additional Notes** Use the space below to provide any project or activity notes, clarifications, requirements or conditions.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**Certifications**

As the PI or RI, as appropriate, I have developed this Technology Control Plan relating to (*insert project name or description*) to adequately safeguard against the export the Controlled Object(s) that will be used or developed or used with this project or activity. I attest to the veracity of this plan and understand that I am responsible to ensure this project or activity is carried out in accordance with this plan. I have discussed this plan and its procedures with my supervisor/ department chair (*name*) and he or she agrees with the plan and its procedures. I agree to update this plan as required and as additional personnel are added to this project and provided notices thereof to the departments/offices stated in this plan. In addition I agree, at all times, to:

1. Ensure that all persons participating in this project are permitted by law to do so and are listed in this technology control plan.
2. Notify my department chair or supervisor and the University’s Compliance officer upon completion of this project and ensure that the disposition of all Controlled Objects is in accordance with this plan.
3. Ensure that all persons participating in this project or activity are listed on this plan and are fully briefed on the requirements of this technology control plan.
4. Inform the my department chair or supervisor and University Compliance Officer immediately upon becoming aware of any violation of this plan or the Federal export control regulations.
5. Promptly notify my department chair or supervisor and provide to the University’s Compliance Officer a copy of all changes to this plan and/or procedures relating to it.

RI/PI Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

RI/PI Printed Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Information Technology Services Manager:** As the ITS manager for this project, I have provided assistance in developing safeguards that will adequately protect both the storage and transmission of export controlled information by electronic means.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Department Chair/Supervisor:** I am aware that the project described above involves materials and/or information which are subject to the Export Control Regulations. The technical control plan described in this document protects all controlled materials and/or information to my satisfaction.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**College Dean/ Department Head:** I am aware that the project described above involves materials and/or information which are subject to the Export Control Regulations. The technical control plan described in this document protects all controlled materials and/or information to my satisfaction.

1) Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**CERTIFICATION FOR SAFEGUARDING EXPORT-CONTROLLED OBJECTS**

(Must be read and signed by all users (including PI or RI) prior to access to an Controlled Objects

**Project or Activity Title:**

**PI/RI Name:**

**Participant Name:**

**Sponsor Name, if any:**

**Description of Controlled Objects:**

**Statement:** I understand that my participation on the project(s) or activity listed may involve the receipt or use of export Controlled Objects, and that it is unlawful to transfer, send or take such Controlled Objects out of the United States. Furthermore, I understand that I may not disclose, orally or visually, or transfer by any means, Controlled Objects to a foreign person located inside or outside the U.S. without a license or applicable exemption as determined by the applicable University department.

A foreign person **means both (i) any foreign entity or group not incorporated or organized to do business in the U.S., and/or (ii) any person who is not a (a) U.S. citizen, (b) permanent resident of the U.S. (i.e., a “green card” holder) or (c) political asylee or refugee status holder. 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 Objects.**

The export Controlled Objects of this project or activity 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>
* jAnyone 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 ORAF for research related screenings and the University Compliance Department for all other screenings.

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 Controlled Objects with others. Unless authorized by the appropriate government agency and notified to that effect by the University Compliance Department, you may not export Controlled Objects to which you have been granted access. If you foresee the need to export any Controlled Object to a foreign country or foreign person (including, but not limited to, any University employees or students) as a part of your research or activity at the University, contact ORAF or the University Compliance Department, as applicable, 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 Objects for any other purpose other than the research or activity referenced below;
* will comply with any and all University export control, security and access policies, procedures and guidelines;
* have been advised by the University that the Controlled Object involved in this project or activity cannot be in any way transferred to other non-US persons without the prior written approval or other written authorization from the University which will determine if a license is required; and
* will not leave or place any Controlled Objects 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 Controlled Objects 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 Controlled Objects 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 this **Certification for Safeguarding Export-Controlled Objects**, and have received a copy of the Technology Control Plan as a part of the University’s export control procedure for the referenced controlled object. I am electing to participate in the research or activity described above, and understand I could be held personally liable if I unlawfully disclose (regardless of form or format) export any Controlled Object to unauthorized persons. I agree to address any questions I have regarding the designation, protection or use of research related export Controlled Objects with ORAF and non-research related objects with the University Compliance Department. This signed form must be provided to PI or RI, as appropriate and submitted with the TCP. Unsigned copies will not be accepted.

**Participant Signature: Date:**

**Printed Name: Title:**