**WASHINGTON UNIVERSITY TECHNOLOGY CONTROL PLAN TEMPLATE**

The purpose of this Technology Control Plan (TCP) is to prevent unauthorized access by foreign nationals to technology controlled for export under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).  This TCP sets forth the security measures the department, principle investigator, and project personnel agree to implement in the performance of this project to prevent unauthorized foreign persons from gaining access to controlled technologies.

**COMMITMENT:**

It is the policy of Washington University to comply fully with all United States laws and regulations, including the laws and regulations governing the export of controlled technologies.  These laws and regulations include without limitation the Export Administration Regulations (“EAR”), the International Traffic in Arms Regulations (“ITAR”), and regulations and orders administered by the Treasury Department’s Office of Foreign Assets Control (“OFAC”) (collectively, the “Export Control Laws”).

**1. Primary Responsible Party (Principal Investigator):**

  Name:
  Department:
  Primary Phone:
  Primary Email:

 **Administrative Contact:**

  Name:
  Department:
  Primary Phone:
  Primary Email:

**2. Identifying information for project**
*[Title, Grant or Contract Number, Sponsor]*

**3. Description of the Item, Technology or Technical Data:**

The nature of the controlled item, technology or technical data is as follows:
*[Identify the item, technology or technical data that is subject to the export control laws.  Include a summary of the project with sufficient detail to explain  the nature of the controlled technology and how it will be used or developed in the performance of this project. Include the relevant ECCN number and/or ITAR classification and other available identifying information for the controlled technology (e.g., equipment manufacturer/model numbers, name/ version of controlled software]*.

**3. Physical Security Plan**Location
Project data and/or materials must be physically protected from access and observation by unauthorized individuals.
 *[Describe the physical location of each sensitive technology/item, to include building and room numbers.]*

Physical Security

*[Provide a detailed description of the physical safeguards that will be put in place to prevent unauthorized persons from accessing the technology/information.  Physical safeguards may include locked doors, locked cabinets/drawers, key card or badge access, escorts and similar physical restrictions.]*

In addition to the foregoing, the following  measures will be observed to prevent inadvertent access by unauthorized foreign nationals to the export-controlled technology/information:

* Hard copies of export-controlled information will be stored in a secure location (e.g., a locked drawer or cabinet) when not in use.
* ​“Restricted Access” signs will be posted at the entrance to laboratories during times that export-controlled technology/information is in use.
* Physical items and WU-generated documents containing export-controlled information will be clearly labelled as “Export Controlled” and secured from unauthorized access.
* Technical data that is printed will be promptly retrieved, and will not be left in the open where unauthorized persons can access it.
* Documents containing export-controlled information will be shredded prior to disposal.

**4. Information Security**

Controlled electronic information must be secured by appropriate measures, such as User IDs, password control, SSL etc. An example would be database access managed via Virtual Private Network (VPN) for authorized persons using 128-bit Secure Sockets Layer (SSL) or other advanced federally approved encryption technology.

*[Describe the structure of your IT security set up at each item/technology location and how you will prevent access by unauthorized persons.]*

*Information security procedures may include the following:*

* Export-controlled files will be password protected or encrypted (128-bit or better).
* Export-controlled technical data shared within the research team must be distributed via secure media and will not be distributed or received via email without encryption.   Cloud services such as Gmail are not secure and therefore may not be used to communicate controlled information.
* All computers containing export-controlled technical data will be locked and password-protected when unattended.
* Use of laptops for data storage will be approved only with additional security procedures.
* Discussions about the project or work product are limited to authorized personnel and are held only in areas where unauthorized personnel are not present.
* Authorized personnel will not leave controlled technology or information where it can be viewed by unauthorized persons.​​
* Removable memory storage devices may be used for data back-up only within the designated secure area.  When not in use, back-up drives must be clearly marked ("Export Controlled") and stored in a designated secured location (e.g. locked drawer or cabinet).
* All electronic storage media must be secured or destroyed upon completion of the project.

**5. Personnel Screening**

*[Identify all personnel who will have access to export-controlled technology/information related to this project.]*

                   Person                                        Nationality
                   Name of Individual                      Indicate “U.S.” if person is U.S. citizen or has green card

This TCP will be amended if personnel changes occur.  All personnel assigned to this project and all visitors afforded access to controlled information or technology must be screened against the U.S. Government’s denied parties lists prior to being afforded such access.  Documentation of screening results will be provided by the Export Control Manager.

**6. Training and Awareness**

All personnel with access to export-controlled technology or information will be briefed on this Technology Control Plan and must certify their understanding of the TCP by signing the attached “Briefing and Certification on the Handling of Export-Controlled Information.”  Additional export control training may be required by the Export Control Manager on a case-by-case basis.

**7. Ongoing Compliance Assessments**

The Export Control Manager may conduct periodic reviews and/or training to assess or improve compliance with the TCP.  Any changes to procedures or personnel identified in this TCP must be approved in advance by the Export Control Manager.  Contact the Export Control Manager with questions or concerns at OVCRExportCompliance@wustl.edu.

**8. Project Termination**

The obligations of this TCP continue as long as the technology/information remains in the University’s possession.  Disposition of export-controlled items, equipment or information should be coordinated with the Export Control Manager.  All records pertaining to the export-controlled technologies/information will be retained in accordance with University policy and all applicable federal regulations.

**9. TCP Annual Review**

All TCPs must be reviewed by the PI on a periodic basis; at a minimum, annually.  This review includes ensuring that all sections of the TCP are up-to-date.  Any changes to personnel or control measures must be reported to the Export Control Manager and a revised TCP developed.

**CERTIFICATION:**
I hereby certify that I have read and understand the terms of this Technology Control Plan.  I agree to follow the procedures set forth herein and to take other actions as necessary to prevent unauthorized access by foreign persons to the controlled technologies.  I understand that I may be held personally liable for civil and criminal penalties, up to and including incarceration, if I disclose any export-controlled information to unauthorized foreign persons.

Printed Name:

Signature:         Date:

Repeat names/signatures/dates for all members of research team

Approved:        Date:
      [Must be approved by the Export Control Manager, Laura Langton, Langton@wustl.edu]