THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Technology Control Plan

Overview:

As Principal Investigator (PI) , your project/disclosed activities has been identified as involving or possible involving the use of Export-Controlled Objects covered under either the Department of State's International Traffic in Arms Regulations (ITAR), or the Department of Commerce's Export Administration Regulations (EAR). It is the policy of The George Washington University (GW) to comply with U.S. export control laws. Controlled Objects[1] 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.

It is unlawful under the EAR to send or take Controlled Objects out of the U.S. or disclose 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.

This document serves as a template for the minimum elements of a Technology Control Plan (TCP) and the safeguard mechanisms that require implementation to protect authorized access, use or disclosure of Controlled Objects and Information. 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.**

I. Background information

Date

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

Technical Description of Controlled Materials Item/Technolog/Software to be used in the Project or Activity

1 Controlled Objects refers to any technical information, data, materials, software, or hardware, (i.e. technology used in this project or activity)

Contract, Grant or other Document Reference to which this TCP Applies (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)

Principal Investigator (PI) and Department

Contact Information

Address:
Telephone:
Email:

II. **Physical Security Plan: All Controlled Objects requiring a license under Export Control 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 concealed from observation by unauthorized individuals by operating in a 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.

a. **Location**: Describe the physical location of each Controlled Object to include building and room numbers:

b. **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.:

III. Project 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 may request the addition or removal of project or activity personnel at any time by completing and submitting a revised TCP to the Office of Research Integrity. Identify every person who is to have authorized access to the Controlled Object item and will be working on this project.

a. Name/ Title/ Date Export Control Training Completed:

b. Name/ Title/ Date Export Control Training Completed:

c. Name/ Title/ Date Export Control Training Completed:

d. Name/ Title/Date Export Control Training Completed:

IX. Information Security Plan: Appropriate controls must be taken to secure all Controlled Objects, including electronic Controlled Objects. Controls may include User ID's, password control, SSL and other GW 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 GW-approved operating systems with the latest security service packs and patches. Please note it is against University Policy to store Export Control Technical information on any cloud storage platform. When travelling with any possible have any equipment, technology, computers or personal devices with information, data or technology subject to export controls should first contact the IT Support Center at 202-994-4948 or email ithelp@gwu.edu for information and support.

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.)

Certification for Safeguarding Export-Controlled Objects

I certify that I am familiar with the GW University Export Control Policy and the export control issues summarized above, and I have read and understand this certification. As the Principal Investigator (PI), I have developed this Technology Control Plan relating to _____ to adequately safeguard against the export of the Controlled Object(s) that will be 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 agree to update this plan as required and as additional personnel are added to this project and provided notices thereof to the offices stated in this plan. In addition, I agree, at all times, to:

1. 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.
2. Inform the Office of Research Integrity immediately upon becoming aware of any violation of this plan or the federal export control regulations.
3. Promptly notify Office of Research Integrity and provide a copy of all changes to this plan and/or procedures relating to it.

PI Signature: _____ Title:_____

PI Printed Name:_____ Date:_____

Participant Signature:_____ Title:_____

Participant Printed Name:_____ Date:_____

Participant Signature:_____ Title:_____

Participant Printed Name:_____ Date:_____

Participant Signature:_____ Title:_____

Participant Printed Name:_____ Date:_____

Participant Signature:_____ Title:_____

Participant Printed Name:_____ Date:_____