**TEMPLATE: Technology Control Plan**

\*\*\*This is a template that may be used to report your Technology Control Plan.\*\*\*

A Technology Control Plan (TCP) is required for all research involving data, material, or technology that falls outside the Fundamental Research Exclusion (FRE) due to contractual restrictions, such as publication or foreign national restrictions, or comes under the authority of the US Department of Commerce’s [Export Administration Regulations](http://www.access.gpo.gov/bis/ear/ear_data.html) (EAR) or the US Department of State’s [International Traffic in Arms Regulations](http://pmddtc.state.gov/regulations_laws/itar_official.html) (ITAR). The US Department of Treasury’s [Office of Foreign Asset Control (OFAC)](http://www.treas.gov/offices/enforcement/ofac/%22%20%5Ct%20%22_blank) is responsible for administering and enforcing economic and trade sanctions against certain nations, entities, and individuals if there is a violation.

Information about EAR and ITAR regulations may be found on UH’s [Division of Research](http://www.uh.edu/research/compliance/export-controls/) website.

Under the EAR and ITAR, it is illegal 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 approval. 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., or not a documented refugee in the U.S. as a protected political asylee or under amnesty. The law makes no exceptions for foreign students.

Relevant technical information, data, materials, software, or hardware such as technology generated from this project, must be secured from use and/or observation by unlicensed non-U.S. citizens. Security measures will be appropriate to the classification involved.

**Technology Control Plan (TCP)**

In accordance with Export Control Regulations (EAR and ITAR), a Technology/Export Control Plan (TCP) is required in order to prevent the unauthorized export of protected items/products, information, or technology deemed to be sensitive to national security or economic interests. This is a basic template for minimum elements of a TCP.

Note: Foreign Nationals may not work on project ineligible for FRE without an export license. Additionally, students (including U.S. citizens) may not work on any project ineligible for the FRE for their thesis or dissertations.

**Technology Control Plan (TCP) Template**

**Principal Investigator and Project Information**

|  |  |  |  |
| --- | --- | --- | --- |
| Date |       | Department |       |
| First Name |       | Last Name |       |
| Email |       | Telephone |       |

Project Number:

Title of Sponsored Project/Activity:

Is there a sponsored research agreement or contract involved?

[ ]  YES [ ]  NO

Is there a nondisclosure agreement or other agreement preceding the sponsored research agreement involved?

[ ]  YES [ ]  NO

**Export-Controlled Information**

Technical description of item, technology, equipment, software to be transferred.

*
*
*
*

**Physical Security Plan**

Project data and/or materials must be physically shielded from the observation by unauthorized individuals. This can be accomplished by conducting the project activities in secured laboratory spaces or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of the “work-in-progress”.

1. 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.

Enter details here.

1. Physical Security. Provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access (e.g. secure doors, limited access, security badges, locked cabinets).

Enter details here.

1. Perimeter Security Provisions. Describe perimeter security features of the location of the protected technology/item.

Enter details here.

**Information Security Plan**

Appropriate measures must be 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.

1. Structure of IT Security. Describe the information technology (IT) setup/system at each technology/item location.

Enter details here.

1. IT Security Plan. Describe in detail your security plan (e.g. password access, firewall protection plans, encryption).

Enter details here.

1. 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.

Enter details here.

1. 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.

Enter details here.

**Item Security**

1. Item Marking. Export controlled information must be clearly identified and marked as such.

Enter details here.

1. 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.

Enter details here.

**Project Personnel**

Clearly identify every person, including national citizenship and country of birth, who is determined to have authorized access to the controlled technology/item. Provide the full names of all faculty, students, staff, visitors and collaborators. Attach additional sheets if necessary.

|  |  |  |
| --- | --- | --- |
| Name (Last, First) | Citizenship | Country of Birth |
|       |       |       |
|       |       |       |
|       |       |       |
|       |       |       |
|       |       |       |
|       |       |       |
|       |       |       |

**Personnel Screening Procedures**

At a minimum, you must review entities and denied parties lists published by the government. This can be done through the federal and state government websites; including but not limited to the following:

* The State of Texas: [Debarred Vendor List](http://www.window.state.tx.us/procurement/prog/vendor_performance/debarred/)
* U.S. General Services Administration: [Excluded Parties List System](https://www.epls.gov/) (EPLS)
* Bureau of Industry and Security
	+ [Denied Person’s List](http://www.bis.doc.gov/dpl/thedeniallist.asp)
	+ [Entity List](http://www.bis.doc.gov/entities/default.htm)
	+ [Unverified List](http://www.bis.doc.gov/enforcement/unverifiedlist/unverified_parties.html)
* U.S. Department of the Treasury: [Specially Designated Nationals List](http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)
* U.S. Department of State
	+ [Debarred List](http://www.pmddtc.state.gov/compliance/debar.html)
	+ [Nonproliferation Sanctions List](http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm)

For assistance, contact the Office of Contracts & Grants at (713) 743-9104.

**Screening Results**

1. Background Checks. Describe types of background checks performed on persons with access to technologies/items (e.g. criminal, driver’s license.

Enter details here.

1. Third Party Contractors. Describe security screening procedures for temporary employment agencies, contractors, etc.

Enter details here.

**Training/Awareness Program**

1. Foreign Nationals. Describe schedules and training for informing foreign national employees of technology access limits.

Enter details here.

2. U.S. Employees. Describe training for U.S. employees with access to controlled technology areas.

Enter details here.

**Self-Evaluation Program**

1. Self-Evaluation Schedule. Describe how often you plan to review/evaluate your TCP.

Enter details here.

1. Audit Checklist. Provide a checklist for items reviewed during self-evaluation audits.

Enter details here.

1. Action Item and Corrective Procedures. Describe your process to address findings in your self-evaluation audits.

Enter details here.

**Technology Control Plan Briefing**

(Must be signed by all persons with access, including PI)

This is to acknowledge that I have read the University of Houston’s Technology Control Plan relating to project name or description and have discussed the procedures with Name (supervisor/PI) and I understand the procedures and agree to comply with the requirements. I agree to update this plan as required and as additional personnel are added to this project.

**Signatures:**

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |       | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |       |
| Name:       | Date | Name:       | Date |
| Title: Principal Investigator |  | Title:       |  |
|  |  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |       | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |       |
| Name:       | Date | Name:       | Date |
| Title:       |  | Title:       |  |

Upon completion of the TCP, the PI must sign and furnish a copy for approval to the Director of Contracts and Grants/Export Control Specialist in OCG, or the Department Business or Research Administrator. Upon approval of the TCP by the Office of Contracts and Grants, the PI may proceed with the handling of export-controlled information. All sections of the TCP must be completed. Retain a copy for lab/department file. If there are any questions while completing the TCP, contact the Contract Officer or the Director in OCG.

Sandy Brown Beverly Rymer

Contract Officer Executive Director

Office of Contracts and Grants Office of Contracts and Grants

(713) 743-1323 (713) 743-5773

snbrown2@uh.edu brymer@uh.edu

NOTE: 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 the control measures need to be reported. The Export Control Specialist will follow-up with the PI on these dates to receive TCP self-audit evaluation results.

**Approved By:**

|  |
| --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Vice President for Research |

*Copies to:*

* *Office of Contracts and Grants (**brymer@uh.edu**)*
* *Project Director*
* *Department Business Administrator/*

*Research Administrator*