**TECHNOLOGY CONTROL PLAN (TCP) – (Insert PI’s last name and year)**

This project/activity involves the use of Export-Controlled Information (ECI). As a result, the project/activity comes under the purview of either the State Department’s International Traffic in Arms Regulations (ITAR) at [here](https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title22/22cfr120_main_02.tpl), or the Department of Commerce’s Export Administration Regulations (EAR) [here](https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear) . Links to information about EAR and ITAR regulations can also be found on ASU’s Office of Research Compliance website (<https://researchcompliance.asu.edu/research-security/>) 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.

Pertinent technical information, data, materials, software, or hardware, i.e.; 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.

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) may be required. If so, this is a basic template for minimum elements of a TCP.

**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 unauthorized exportation 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.

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

**Period of Performance: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| **Title of Sponsored Project/Activity:** | **Also include FP# and or AWD# Task** |

|  |  |
| --- | --- |
| **Technical Description of Item, Technology, Equipment, Software To Be Transferred:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |  |
| --- | --- |
| **Principal Investigator (PI):** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Phone:** |  | **E-Mail:** |  |

1. **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”)
	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):

|  |
| --- |
|  |

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

|  |
| --- |
|  |

* 1. **Perimeter Security Provisions** (describe perimeter security features of the location of the protected technology / item):
1. **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 as may be required by federal sponsor, e.g. NIST 800-171 or CMMC certified systems).
	1. **Structure of IT security** (describe the information technology (IT) setup / system at each technology / item location:

|  |
| --- |
|   |

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

* 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.):

|  |
| --- |
| We will notify all sponsors associated with the specific item immediately. We will remove access of the terminated employee. Research Operations shall be notified for all changes in personnel supporting this Project to control access and will update the TCP accordingly.  |

* 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 undersigned agreements that fully respect the non-U.S. citizen limitations for such disclosures. Describe your plan for protecting export-controlled information in conversations):

Discussion of export-controlled information in any form will be limited to authorized users and will occur only in closed-door meetings in an approved users identified location. Discussion of export-controlled information or data will not take place with anyone who has not been approved and received training through the TCP approval process.

Any discussions with subcontractors regarding controlled technical data shall be governed by federal government export-controlled requirements flowed down in the subcontracts.

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

|  |
| --- |
| All controlled items including controlled technical data will be marked as required by federal government export requirements or per sponsor direction.  |

* 1. **Item Storage All controlled items will be marked and stored in secured location. (**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):

|  |
| --- |
|  |

1. **Project Personnel** (clearly identify every person (including their national citizenship) who is determined to 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:** |  |

1. **Personnel Screening Procedures**

**At a minimum, you must review entities and denied parties lists published by the government. This can be done for you by Export Control. Please contact for assistance at** **export.control@asu.edu****.**

* 1. **Background Checks** (describe types of background checks performed on persons with access to technologies / items, i.e., criminal, drivers license, etc.):

|  |
| --- |
| New Project personnel will be screened in-accordance-with ASU HR requirements and against federal government entities lists. Sponsor’s approval will be obtained if required by the award. |

* 1. **Third Party Contractors** (describe security screening procedures for temporary employment agencies, contractors, etc.):

|  |
| --- |
| Any third-party contractors or participants that will be engaged during the project will be reviewed to determine if export control requirements apply to the proposed work. If so, subcontractors will be screened against federal government entities lists and applicable federal government export-controlled requirements will be flowed down. |

1. **Training / Awareness Program**
	1. **Foreign Nationals** (describe schedules and training for informing foreign national employees of technology access limits):
	2. **U.S. Employees** (describe training for U.S. employees with access to controlled technology areas.

|  |
| --- |
| All Project are required to take the following training prior to beginning work on this project: * CITI - Export Compliance
* CITI - Research Security (required annually)
* DoD Mandatory Controlled Unclassified Information (CUI) Training - [DoD Mandatory CUI Training](https://www.cdse.edu/Training/eLearning/IF141/)
* Export Compliance annual refresher (ASU ICRA will provide training)

Contact export.control@asu.edu for information on how to complete the CITI Training. |

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

PI will review and evaluate the TCP annually. The PI will notify Research Operations/Export Control of any needed updates or changes required. After taking the CITI Export Compliance training, ICRA will provide the annual Export Control refresher training course.

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

|  |
| --- |
| 1. List of all personnel that had access to project information2. Log of where the information/material was stored3. Review of security plan |

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

|  |
| --- |
| Audit checklist will consist of the following: list of personnel that had access to project information, log of where the information/material was stored and a review of security plan. Audit reports will be shared with the Office of Research Compliance and other designated officials. If corrective actions are needed, the Office of Research Compliance will be consulted. |

**TECHNOLOGY CONTROL PLAN CERTIFICATION FOR HANDLING EXPORT CONTROLLED INFORMATION**

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

This is to acknowledge the following:

1. I have read this Arizona State University Technology Control Plan (TCP) relating to (**insert project name of description**) and the **GUIDELINES FOR THE PROTECTIVE SECURITY OF TECHNICAL INFORMATION/DATA, MATERIALS AND EQUIPMENT THAT ARE EXPORT CONTROLLED** below.

2. I havediscussed this TCP and the GUIDELINES with my supervisor/PI (**name**) and I understand the requirements and agree to comply with them.

3. I understand that I could be held personally liable if I unlawfully disclose export-controlled technical data to foreign persons and agree to take measures to prevent unauthorized foreign persons from having access to or using any export-controlled technical data I may receive.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | Signature | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Title |  |
|  | Printed Name |  | Date |  |
| 2 | Signature |  | Title |  |
|  | Printed Name |  | Date |   |
| 3 | Signature |  | Title |  |
|  | Printed Name |  | Date |  |
| 4 | Signature |  | Title |  |
|  | Printed Name |  | Date |  |

Retain copy for lab/department file

Copies to: Export.Control@asu.edu \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_

 Lab Director/Department Chair Heather C. Clark, Chief Research Compliance Officer, Empowered Official

 Research Compliance Office

**GUIDELINES FOR THE PROTECTIVE SECURITY OF TECHNICAL INFORMATION/DATA, MATERIALS AND EQUIPMENT THAT ARE EXPORT CONTROLLED.**

Project security is the responsibility of the Principal Investigator (PI). Specifically, technical information, data, materials, software or hardware, i.e., technology, generated from an export-controlled grant/contract or subgrant/subcontract will be secured from use and observation by non-U.S. persons. Examples of some methods to provide this security are as follows:

• Project Personnel – The use of access badges may be necessary as an aid to identify personnel whose access to project facilities and work in progress is authorized.

• Laboratory “work in progress” – Project data and/or materials must be physically shielded from observation by unauthorized individuals operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.

• Work Products – Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets, preferably located in rooms with key – controlled access. The specific manner of storing hard copy work products must be described in the Technology Control Plan.

• Equipment or internal components – Such tangible items and associated operating manuals and schematic diagrams containing identified “export controlled” technology are to be physically secured from unauthorized access.

• Electronic communications and databases – Access to, use of, and/or electronic communications of export-controlled data or information must be only via ASU approved means. Technology Control Plans must describe specific information security requirements.

• Conversations – Discussions about the project or work products are limited to the identified project personnel and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only conducted under a signed confidentiality agreements and fully respect the non-U.S. limitations for such disclosures.

Principal Investigators are reminded that, per ASU Research and Sponsored Projects Manual- RSP 406 Publication (<https://policy.asu.edu/>), sponsor restrictions on the publication or public disclosure of technical information, data, materials, or software generated under an export-controlled grant or contract must have a **publication waiver** approved by the KE Office of Research Compliance authorized official prior to commencing any work.

The penalty for unlawful export and disclosure of Export-Controlled Information under the ITAR, EAR or OFAC can be severe. Criminal and civil penalties can be monetary (e.g. up to $1 million per violation), prison time (e.g. up to 20 years), or both, and Debarment. For more information see [ITAR penalties,](https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=e1999c7fdb78d300d0a370131f96193d)  [OFAC CIVIL penalties and Enforcement Information](https://ofac.treasury.gov/civil-penalties-and-enforcement-information), [EAR penalties](https://www.bis.doc.gov/index.php/enforcement/oee/penalties).

 **Definitions:**

Foreign National: A “foreign national” is anyone who is not a U.S. citizen, a lawful permanent resident of the U.S. (i.e., a “green card” holder) or a “protected individual” as defined in 8 U.S.C. §1324b(a)(3) (e.g., refugees or persons seeking asylum in the U.S.). A foreign national also means any foreign corporation, business association, partnership, or any other entity or group that is not incorporated or organized in the U.S., including international organizations, foreign governments and agencies, and subdivisions of foreign governments. Where a foreign national is a citizen of more than one foreign country or has citizenship in one foreign country and permanent residence in another, the general rule is that the last permanent resident status or citizenship obtained governs.

U.S. Person: Includes United States citizens and “Green-Card” holders, permanent resident aliens. It also includes any corporation, business association, partnership, society, trust, or any other entity organization or group that is incorporated to do business in the United States.