

**University of South Alabama  
Technology Control Plan**

**Principle Investigator:**

**Department:**

**Project Title:**

**Sponsor:**

**Date:**

**This plan has been approved and adopted by the University of South Alabama**

---

**Lynne Chronister, Empowered Official  
Vice President for Research, University of South Alabama**

## **Policy Statement**

The University of South Alabama will comply with all applicable export controls as established by federal regulations. Export controls restricting a foreign national's participation in university research within the United States generally do not apply to the conduct or results of fundamental research. Such practices, as defined and stipulated, include openly conducted basic and applied research in science and engineering that is not subject to access, dissemination, or participation restrictions of any sort.

However, in the case of shipments of tangible items, software, or information controlled by federal agencies outside the U.S., travel of persons outside the U.S, or projects that accept restrictions based upon nationality or publication, USA has a responsibility to:

1. Conduct a technical review; and if necessary
2. Document an express determination that an exception to export licensing is applicable; or
3. Obtain an export license; or
4. Develop a Technology Control Plan with the Principal Investigator

## **Background**

Since the 1940's export controls set forth in regulations have been administered by three main federal agencies to impose access, dissemination, and participation restrictions on the transfer (export) and retransfer (re-export) of "controlled" information, software, technology, and export and re-export of tangible items. Such efforts are made to prevent terrorism, curtail export of technologies that assist the military potential of adversaries, comply with trade agreements, and prevent development of nuclear, chemical and biological weapons.

An "export" is defined very broadly to include an oral or written disclosure of information, visual inspection, or actual shipment outside the U.S. of technology, software/code or equipment to a foreign person or entity. Transfer of any of the above described is also applicable to foreign persons or entities within the United States defined as a "deemed export".

The US Commerce Department must issue an export license, or provide an exception to or exclusion from license requirements before any controlled tangible item, software, or information on the Commerce Control List (CCL)

([http://www.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html)) (may be exported or re-exported. Likewise, if the item in question is on the US Munitions List (USML)

([http://www.pmddtc.state.gov/regulations\\_laws/itar\\_official.html](http://www.pmddtc.state.gov/regulations_laws/itar_official.html)) the US State Department must issue or provide for any exceptions to or exclusion from licensing requirements. Sending controlled items or information to a sanctioned country as defined by the Office of Foreign

Assets Control (OFAC) (<http://www.ustreas.gov/offices/enforcement/ofac/faq/answer.shtml#9>) is generally prohibited in all forms.

Disclosure of export controlled technology to Foreign Persons may be considered an export under the International Traffic in Arms Regulations (ITAR, 22 CFR 120-130) and/or Export Administration Regulations (EAR 15 CFR 734) and may be subject to a Department of Commerce or Department of State license or agreement. An export may occur by passing of information or material that is export controlled even within the U.S if it is to a foreign national, this is referred to as a deemed export.

## **Purpose**

The purpose of this Technology Control Plan (TCP) is to ensure that technical information and/or technical data or the use of controlled equipment which is not specifically exempted as Fundamental Research and/or Educational Information by EAR or ITAR is not transferred to Foreign Persons (including employees, visitors or students) unless approved by a government license. The Office of Research Compliance and Assurance (ORCA) is responsible for evaluating a proposed project for the purpose of determining the specific security measures needed to prevent the unauthorized export of restricted technical data, technology or information, as required by export control laws and university policy. The Principal Investigator and staff involved in the conduct of the project are responsible for adhering to the TCP, and the ORCA is responsible for overseeing their compliance with the TCP. A [TCP template](#) is available at the end of this document.

## **Key Definitions**

Controlled Item(s): Includes any information, technical data, oral/written disclosure, or visual inspection of items or descriptions contained within federal regulatory lists governing export controls. These lists are principally the Commerce Control List and United States Munitions List.

Deemed Export: Release of controlled technology to a foreign national in the United States is “deemed” to be and export as if it were released to the foreign national’s country of origin.

Empowered Official: A U.S. person who is legally empowered to sign export license applications or other requests for approval on behalf of the University of South Alabama who understands the provisions and requirements of the various export control statutes, regulations, and penalties for violating export control laws. The Vice President for Research is the “Empowered Official” for the University.

Export: Defined very broadly to include an oral or written disclosure of information, visual inspection, or actual shipment outside the U.S. of technology, software/code or equipment to a foreign person or entity.

Foreign National: Any person who is not a U.S. citizen, lawful permanent resident alien (“green card holder”), refugee, protected political asylee, or someone granted temporary residency under amnesty or Special Agricultural Worker provisions. Also, any foreign government or any foreign corporation or entity that is not incorporated or organized to do business in the U.S.

Fundamental Research: Basic or applied research in science and engineering performed or conducted at an accredited institution of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community.

University research will not be considered fundamental research if:

- 1) The University or its researchers accept other restrictions on the publication of scientific and technical information resulting from the project or activity, or
- 2) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

Publication or Dissemination Restrictions: Acceptance in research and development of any prohibition or approval authority over publication or any other dissemination of research results, except, sponsor or collaborator may include provisions for review of results, with a short review period to remove some sponsor/collaborator business proprietary or pre-patentable information.

Release: Technology or software is “released” for export through: (i) visual inspection by Foreign Nationals of U.S.-origin equipment, facilities, technology, or documentation; (ii) oral or written exchanges of information in the United States or abroad; (iii) the application to situations abroad of personal knowledge or technical experience acquired in the United States; (iv) or physical export of controlled item.

Technology and Technical Data: These terms refer to technical information beyond general and basic marketing materials about a controlled commodity. The terms do not refer to the controlled equipment or commodity itself, or to the type of information contained in publicly available user manuals. Rather, the terms “technology” and “technical data” mean specific information necessary for the development, production, or use of a commodity. The information usually takes the form of blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering specifications, and documentation.

Technical Review: Refers to the initial review by the university Office of Research Compliance and Assurance (ORCA) of an export, tangible or information, for determination of if the item in question falls under the purview of export controls. Results of the review and further action required are logged and monitored by ORCA.

Technology Control Plan (TCP): A plan prepared by Principal Investigator and approved by the ORCA, for ensuring that there will be no unlawful export of restricted commodities, defense articles, software, data, technology, or technical data in a Sponsored Project without an appropriate government approval.

## **TCP Template**

### **Project Specific Information**

**{Project Title}**

#### **Commodity Jurisdiction and Classification *(to be completed jointly by the PI and Office of Research Compliance)***

This project is subject to export control restrictions under *(fill-in the specific EAR or ITAR ECCN or Category.)* The applicable category/categories are below:

*Insert detail of EAR and or ITAR listing*

As a result of this determination, the Principal Investigator has adopted a TCP to ensure that controlled defense services, articles, technical data, and dual use items, hereafter referred to as “controlled items”, are adequately protected from disclosure to foreign persons that do not have an approved license, valid license exception from the government, or other government approval. Any data/or research results generated from the controlled items **will also** be treated at controlled items. The plan addresses physical security, information security, personnel screening procedures and training and is detailed below.

*Insert the purpose of this project is to list objectives here.*

#### **Security Overview**

“One Lock” is the principle of securing controlled items by using at least one mechanism to prevent disclosure to unauthorized persons. This is the minimum requirement for safeguarding the controlled items. Methods for obtaining at least “one lock” are described in the physical and information security sections below. It is the responsibility of the project personnel to safeguard the controlled items at all times by having “one lock” in place

#### **Physical Security**

##### Work Area

The minimum security requirement for a controlled item work area is set forth in the National Industrial Security Program Operating Manual (NISPOM); section 5-305 “Restricted Areas”. (<http://nsi.org/Library/Govt/Nispom.html>) The restrictions shall have a clearly defined

parameter, which is adequate to protect against oral and visual disclosure of the controlled items. Physical barriers are strongly recommended but are not required as long as oral and visual disclosure can be prevented. Project personnel within the Restricted Area shall be responsible for challenging all persons who may lack appropriate access authority.

### Storage

All controlled items will be secured in a locked storage container when not in the personal possession of the approved project personnel. All controlled items shall be marked "controlled" on an individual basis.

*Insert any additional physical security measures unique to the named project.*

## **Information Security**

### Computer

Approved project personnel are the only designated users of computers and a valid account and password must be provided to gain access. Only approved project personnel retain this login information and no other login accounts are created. Both failed and successful logins are logged internally.

### Data Storage and Transmission

External portable hard drives or flash drives are strongly recommended for data storage. These storage devices can easily be locked in a storage container when not in use. It is suggested that these drives are password protected or encrypted. For data storage on drives with network access or backup servers, the controlled technical data files must be secured by encryption or password protection. Emails shall not contain controlled technical data files unless both send and receive email locations are encrypted and for use between approved project personnel.

*Insert any additional information security measures unique to the named project.*

## **Project Personnel Screening Procedures**

### Personnel

All personnel involved in the conduct of the project will review this plan and complete Attachment A: [\*Acknowledgment of Technology Control Plan\*](#). All project personnel have attended or will attend export control training provided by ORCA. Personnel who have not had training before having access to controlled items will be signed up for the next available training session. All project personnel are made aware of their responsibilities to prevent either active or inadvertent disclosure of controlled items. All project personnel will be screened against applicable parties' access lists and will have their nationality screened by ORCA.

### Principal Investigator

The PI shall review and sign Attachment B: [\*Non-Disclosure Statement\*](#). The PI has attended or will attend export control training provided by ORCA. The PI is made aware of their responsibilities to prevent either active or inadvertent disclosure of controlled items and of civil and criminal penalties (including prison sentences of up to 10 years and fines of up to \$1M) for failure to comply with United States export control rules. The PI will notify ORCA before adding additional personnel to a project having access to export controlled items.

#### Principle Investigator: Foreign National

In the event that the PI is a foreign national with a full time residence in the United States for the duration of the research, and not from a restricted country, under the ITAR 22 CFR 125.4 (b)(10) ([http://www.pmddtc.state.gov/regulations\\_laws/documents/official\\_itar/ITAR\\_Part\\_125.pdf](http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_125.pdf)) that individual is subject to an employment exemption will receive Attachment C: [\*Bona Fide Employee letter\*](#). The PI is made aware of their responsibilities to prevent either active or inadvertent disclosure of controlled items and of civil and criminal penalties (including prison sentences of up to 10 years and fines of up to \$1M) for failure to comply with United States export control rules. The PI will notify ORCA before adding additional personnel to a project having access to export controlled items.

#### **Training**

Training modules on the basic rules of export controls as they apply to a university research setting, and in particular the named project will be offered by the ORCA at periodic intervals. Instruction will include familiarization to the regulations of the EAR, ITAR, and Office of Foreign Assets Control (OFAC), as well as, expectations of compliance to said regulations. All project PIs and participants are expected to complete training prior to, or in a timely fashion after, funding.

#### **Publication Risks**

In most cases restricted research will contractually require that project personnel shall not release or disseminate any information pertaining to the project without the prior written approval of the sponsor, excluding information already in the public domain. In the rare case there is not a contractual publication restriction and the project involves controlled items, research results and publications generated from the controlled items are still subject to the approval of the sponsor. Therefore, publications of projects that involve controlled items are subject to the approval of the sponsor and should be considered prior to employing graduate students or tenure track faculty. Publications (including but not limited to theses, dissertations, and journal publications) may be delayed or denied based on approval of sponsor.

#### **Project Completion Requirements**

Upon completion of a restricted research project, all controlled items will be disposed of or stored properly. The secure storage requirements set forth in the previous sections remain the same after completion of the project. Hard copies will be disposed of by shredding. Electronic files will be "wiped."

**Special Notes**

*This section is reserved for any additional special notes of information pertaining to the specific project.*

**Self Assessment/Auditing**

The PI and department shall notify ORCA (1) each time an additional person is added to the project so that they can be screened and trained, and (2) when the scope of the project changes. The PI will certify and the *(insert department)* shall approve that the project is being carried out in compliance with this TCP. The PI and project participants are subject to random audits conducted by ORCA to assure adherence to aforementioned policies. Any items of issue will be reported to the USA Empowered Official. The Principal Investigator shall annually certify to ORCA that they are complying with the TCP for each export controlled project for which they are responsible. Attachment D: [Annual Certification of Adherence to Technology Control Plan](#) will be signed as confirmation.

**Submitted:**

_____	_____	_____
Principal Investigator	Department	Date

**Acknowledgment of Immediate Supervisor:**

_____	_____	_____
Supervisor Signature	Department	Date

**Attachment A**

**Acknowledgement of Technology Control Plan  
for the University of South Alabama:  
Project Participants**

Project Name:

Sponsor:

PI:

I hereby certify that I have read and understand the provisions of the above Technology Control Plan, as well as, understand that I could be held personally liable if I unlawfully export, regardless of form or format, controlled items to unauthorized persons or entities.

Print Name: \_\_\_\_\_

Department: \_\_\_\_\_

US Citizen\_\_\_ US Permanent Resident (Green Card)\_\_\_ Foreign National\_\_\_

Country of Origin\_\_\_\_\_

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

Date: \_\_\_\_\_

## **Attachment B**

### **Non-Disclosure Statement**

I, \_\_\_\_\_ (insert name of individual) acknowledge and understand that any technical data or defense services related to defense articles on the U.S. Munitions List or disclosure of information pertaining to dual use items on the Commerce Control List to which I have access or which is disclosed to me in the course of my (insert which every term is applicable, *employment, assignment, or visit*) by/at the University of South Alabama is subject to export control under the International Traffic in Arms Regulations (title 22, code of Federal Regulations, Parts 120-130) and/or the Export Administration Regulations (title 15, code of Federal Regulations Parts 730-774). I hereby certify that such data or services will not be further disclosed, exported, or transferred in any manner to any foreign national or any foreign country without prior written approval from the United States government or application of lawful exceptions. All listed above as in accordance with the U.S. export controls and customs regulations.

\_\_\_\_\_  
Print name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

## **Attachment C**



### **Bona Fide Employee Letter**

*Applicable to University of South Alabama employees who are exempt of export control restrictions as a Bona Fide employee of the University*

Dear:

You are hereby notified that as \_\_\_\_\_ (*participant/principle investigator*) in the Sponsored Project \_\_\_\_\_ (*name of project*) you will be producing International Traffic in Arms (ITAR) export control restricted experimental or developmental items specifically designed or modified for military application or specifically designed or modified for use with a military system and associated technical data. In accordance with ITAR 22 CFR 125.4(b)(10), the ITAR-restricted defense articles or technical data may not be transferred to foreign persons without the prior written approval of the Office of Defense Trade Controls. Prohibited technical transfers include oral, visual, written or electronic disclosure, as well as, transfer of physical custody. Violations of the ITAR can result in criminal penalties for up to 10 years in prison and one million dollars (\$1,000,000) in fines, and civil penalties of up to \$500,000 in fines and forfeiture (22 CFR 127-1 through 127-12). If you have questions about this export control restriction, please call Mary Anne Connors (251-460-6509).

Sincerely,

Mary Anne Connors  
Assistant Director of Research Compliance and Assurance  
University of South Alabama

## **Attachment D**

### **Annual Certification of Adherence to Technology Control Plan**

I, \_\_\_\_\_ (*insert name of individual*) understand that the project (*insert project name*) of which I am Principle Investigator is subject to United States Export Controls Law. I certify that this project remains in compliance with the Technology Control Plan developed between myself and the Office of Research Compliance and Assurance (ORCA) on (*insert date*). In congruence with that instruction any technical data or defense services related to defense articles on the U.S. Munitions List or disclosure of information pertaining to dual use items on the Commerce Control List to which I have access or to which is disclosed to me in the course of my project at the University of South Alabama is subject to export control under the International Traffic in Arms Regulations (title 22, code of Federal Regulations, Parts 120-130) and/or the Export Administration Regulations (title 15, code of Federal Regulations Parts 730-774). I hereby certify that such data or services will not be further disclosed, exported, or transferred in any manner to any foreign national or any foreign country without prior written approval from the United States government or application of lawful exceptions. Furthermore, any deviation from the Technology Control Plan referenced above will be lawfully developed and amended with the assistance of ORCA. All listed above as in accordance with the U.S. export controls and customs regulations.

\_\_\_\_\_  
Print name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

