THE RESEARCH FOUNDATION
The State University of New York

Export Management System: Technology Control Plan
May, 2009

Introduction

Requirements

Signatures & Certifications

Appendices

Export Management System: Technology Control Plan
Introduction

Overview
A Technology Control Plan (TCP) outlines the procedures used by the Research Foundation (RF) to prevent the unauthorized export of and/or access to controlled items, technology or data. A TCP:

- Is needed when an export license, disclosure or situation requires one.
- Assures an organization's due diligence and compliance with U.S. federal government Export Administration Regulations (EAR) and International Traffic in Arms (ITAR) Regulations (export control regulations).
- Protects the principal investigator, the research program, the campus, the RF and the university.

This document provides a TCP template and includes the following essential elements. The campus sponsored research office and principal investigators must use the essential elements in a TCP, as they are applicable to a specific export control license, disclosure, or situation.

Introduction
- Overview
- Responsibilities of appropriate persons/offices

Requirements
- Corporate commitment to export controls compliance
- Basic information and description of the situation
- Physical security plan
- Information technology (IT) security plan
- Item security plan
- Project personnel and screening
- Training and awareness program
- Compliance assessment

Certifications & Signatures
- Foreign nationals/persons for deemed exports
- Other project persons/entities
- Principal investigator
- Operations manager/empowered official
- Prepared by

Appendices
- A - Key definitions

It is important for persons applicable to the TCP to be informed regarding self disclosure and that any knowledge of noncompliance or violation of the TCP or export control regulations must be reported to the campus operations manager/empowered official. Any person reporting in good faith noncompliance or violation will not have adverse actions taken against them as a result of making such a report.

Export Management System: Technology Control Plan
Introduction

Responsibilities
The following table identifies the responsibilities of the appropriate persons/offices for completing the Requirements section of the TCP.

Persons/Offices	Responsibilities	Page
Research Foundation Central Office	Corporate commitment	3
Sponsored Research Office	Basic information	4
Sponsored Research Office	Background & description of the situation	7
Principal Investigator	Physical security plan	8
Principal Investigator	Information technology security plan	9
Principal Investigator	Item security plan	10
Sponsored Research Office	Project personnel & screening	11
Sponsored Research Office	Training & awareness program	12
Sponsored Research Office	Compliance assessment	13
Sponsored Research Office	Obtaining the required signatures (e.g., foreign nationals/persons for deemed exports, other project persons/entities, principal investigator, operations manager, empowered official, prepared by) on the certification pages.	14

Export Management System: Technology Control Plan
Requirements

Corporate Commitment to Export Controls Compliance
The Research Foundation of State University of New York (RF) is committed to assuring compliance with the U.S. federal government export control regulations.

The ***RF Central Office*** is responsible for:

- Developing and implementing an export management system for the sponsored programs conducted at the State University of New York campus locations.

- Providing assistance to the decentralized and centralized campus locations with their local export controls programs; and the development of license requests and Technology Control Plans (TCP) - as requested and as appropriate.

Export Management System: Technology Control Plan
Requirements

Basic Information

In situations where a Technical Control Plan (TCP) is required:

- The campus sponsored programs/research office is responsible for implementing the TCP.
- The campus operations manager/empowered official are responsible for assuring compliance with the TCP.

The ***sponsored research office*** is responsible for completing this section

Sponsored Program	
Proposal Number	
Award Number	
Award Title	
Sponsor Name	
Award Amount	
Award Period	
Export Control License (if applicable)	
Federal Agency Name	
License Number	
License Date	
License Requirements	

Export Management System: Technology Control Plan
Requirements

Basic Information (continued)

Principal Investigator	
Name	
Title	
Department	
Phone Number	
E-mail Address	
Operations Manager	
Name	
Title	
Office	
Phone Number	
E-mail Address	
Empowered Official	
Name	
Title	
Office	
Phone Number	
E-mail Address	
Research Administrator	
Name	
Title	
Office	
Phone Number	
E-mail address	

Background and Description of the Situation
The background and description of the specific situation must be provided to identify the purpose of the TCP.

The ***sponsored research office*** is responsible for completing this section.

Describe the background of the specific situation (e.g., export of a controlled item, access to controlled technology/data, etc.).

Describe the controlled item, technology or data; including scientific information that is provided by the principal investigator.

Physical Security Plan
The controlled item, technology or data must be physically protected from unauthorized persons by assuring a secure physical location, security plan, and perimeter security provisions; as applicable to the situation.

The ***principal investigator*** is responsible for completing this section.

Describe the physical location, including building and room numbers. In addition, a schematic of the location is highly recommended.

Describe the physical security plan to protect the controlled item, technology or data from unauthorized access (e.g., security systems, badge systems, escorts, visitor logs, building access restrictions, etc.).

Describe the perimeter security features for the location.

Information Technology Security Plan
Controlled/sensitive digital research data must be appropriately protected through information access controls that assure information technology (IT) security. Additional considerations for IT security include, but are not limited to: Data discard procedures, system backups, the personnel who will have access, transmission procedures, sanitizing computers upon project completion, and use of laptops for storage.

The ***principal investigator*** is responsible for completing this section.

Describe the following as applicable to the situation:

IT Security Structure: The IT setup, system and location.

IT Security Plan: The use of passwords, firewalls and encryption.

Verification of Item/Technology Authorization: The ability to access export controlled information for new persons working on the project as well as for terminated employees.

Conversation Security: The practical/reasonable plan for protecting export controlled information in conversations, for example:

- Discussions about the controlled technology or data, and any aspects of the project that are impacted by its use, will be limited to those between/among the principal investigator, U.S. citizens, permanent residents, and authorized foreign nationals. Unauthorized persons must not be involved in these discussions.

- Discussions about the controlled technology or data, and any aspects of the project that are impacted by its use, with third parties (e.g., subcontractors, consultants) will be conducted only when a signed agreement is in place, if applicable.

Graduate Thesis: Any graduate student thesis research that could result in the development of a controlled item, technology or data.

End-of-Project Security Plan: How the controlled technology or data, including papers and hard drives, will be disposed (e.g., sanitizing, shredding, wiping software, etc.).

Termination Plan: How the IT security plan will be invoked when a principal investigator of a project with controlled technology or data leaves the campus/university.

Item Security Plan
The controlled item, technology or data must be clearly identified and marked, and be physically and securely stored.

The ***principal investigator*** is responsible for completing this section.

Describe the following as applicable to the situation:

Item Marking: How the controlled item, technology or data will be labeled and/or marked to clearly indicate that it is controlled; including the legend that should be stamped/added.

Item Storage: How the controlled item, technology or data will be securely stored (e.g., locked cabinets, rooms with key-controlled access, etc.). In addition, controlled equipment or internal components and associated equipment operating manuals, schematic diagrams, and internal components will need to be physically and securely stored**.**

Project Personnel and Screening
All project personnel, and other persons, who have access to the controlled item, technology or data must be identified.

The ***principal investigator*** and ***sponsored research office*** are responsible for completing this section.

Describe the following as applicable to the situation:

Principal Investigator
List of Project Personnel: Maintain a list of project personnel (e.g., names, addresses, nationalities) to identify all of the persons (e.g., research assistants, collaborators, students, post-doctorals) working on the project throughout the sponsored award period. The list should be regularly maintained to assure it provides a current status of project personnel.

List of Third Parties: Maintain a list of third parties (e.g., subcontractors, employment agencies, associated organizations/businesses, etc.) with access to the controlled item, technology or data working on the project throughout the sponsored award period. The list should be regularly maintained to assure it provides a current status of third parties.

Sponsored Research Office
Screen Project Personnel: The names of project personnel must be screened using the MSR eCustoms compliance tool, Visual Compliance/Research Edition via the restricted party screening feature. In addition, restrictions on foreign nationals must be documented using the compliance tool, via the controlled goods analyst (commerce control list/CCL), export commerce control number/ECCN). All of the compliance tool results must be reviewed and documented.

Screen Third Parties: The names/entities of third parties (e.g., subcontractors, employment agencies, associated organizations/businesses, etc.) with access to the controlled item, technology or data; must be screened using the MSR eCustoms compliance tool; and the results reviewed and documented.

Training and Awareness Program
All project personnel, and other persons, who will have access to the controlled item, technology, or data must participate in a training and awareness. The campus will determine the type of program that is appropriate.

The ***sponsored research office*** is responsible for completing this section.

Describe the training and awareness program that will be conducted, as applicable to the situation.

Compliance Assessment
A critical component of the TCP is a self-evaluation schedule, internal assessment, and corrective action plan to assure compliance with the purpose of the TCP.

The ***sponsored research office*** is responsible for completing this section.

Describe the following as applicable to the situation:

Self-Evaluation Schedule: How often the TCP will be reviewed/evaluated.

Internal Assessment: A checklist of the items from the TCP that will be reviewed/evaluated during the internal assessment, and document the findings.

Corrective Action Plan: The findings that require a corrective action, and identify, document, and incorporate the corrective actions in the TCP.

Export Management System: Technology Control Plan
Certifications & Signatures

Foreign Nationals/Persons Certification For Deemed Exports

This certification must be used when the situation involves deemed exports – the release/access of a controlled item, technology, or data to a foreign national/person inside the U.S.

If more than one foreign national/person is connected with this TCP, multiple signatures should be listed on this page, a separate TCP is not required.

Non-Disclosure Statement

To assure the protection of the export controlled items (e.g., equipment, technology, data) identified under this Technology Control Plan (TCP), I agree not to release and/or disclose any information obtained in connection with my use of the controlled items required for the applicable sponsored program. I also agree to assure compliance with the essential elements of the TCP.

Foreign National/Person Signature:

Signature: _____Date: _____

Printed Name: _____

Title and Department: _____

Country of Origin: _____

Export Management System: Technology Control Plan
Certifications & Signatures

Other Project Persons/Entities

This certification must be used when the situation involves the use of a controlled item, technology, or data outside of the U.S. – by other persons/entities working on the project as appropriate to the sponsored program award.

If more than one other project person/entity is connected with this TCP, multiple signatures should be listed on this page; a separate TCP is not required.

Non-Disclosure Statement

To assure the protection of the export controlled items (e.g., equipment, technology, data) identified under this Technology Control Plan (TCP), I agree not to release and/or disclose any information obtained in connection with my use of the controlled items required for the applicable sponsored program; and agree not to reexport the controlled items to another country, person, or entity. I also agree to assure compliance with the essential elements of the TCP.

Other Project Person Signature:

Signature: _____Date: _____

Printed Name: _____

Title and Department: _____

Country of Origin: _____

Other Project Entity Signature:

Signature: _____Date: _____

Printed Name: _____

Title and Department: _____

Entity Name: _____

Complete Address: _____

Export Management System: Technology Control Plan
Certifications & Signatures

Principal Investigator Certification

It was determined that a Technology Control Plan (TCP) is required for the applicable sponsored program. This acknowledges that I have read and understand the export controls information for principal investigators on the RF's Web page, that I understand I could be held personally liable for certain export control violations, and that I agree to assure compliance with the essential elements of the TCP.

Principal Investigator:

Signature: _____Date: _____

Printed Name: _____

Title: _____

Export Management System: Technology Control Plan
Certifications & Signatures

Certification
The undersigned acknowledge that they have read and understand the purpose of this Technology Control Plan (TCP), and agree to assure compliance with these requirements.

If the Operations Manager is also the Empowered Official, only his/her signature as the Operations Manager is required.

Operations Manager or Delegate:

Signature: _____Date:_____

Printed Name: _____

Title and Department: _____

Empowered Official (if different from Operations Manager):

Signature: _____Date: _____

Printed Name: _____

Title and Department: _____

Export Management System: Technology Control Plan
Certifications & Signatures

Certification
The undersigned acknowledge that they have prepared the TCP with the information as provided by the principal investigator and the sponsored research office.

Prepared By:

Signature: _____Date:_____

Printed Name: _____

Title and Department: _____

Appendix A

Key Definitions
The following is a short appendix of some of the key definitions for export control terms.

- What are export controls?
  The federal definition of export controls is U.S. federal government laws and regulations that require federal agency approval before the export of controlled items, commodities, technology, software or information to restricted foreign countries, persons and entities (including universities). There are three federal government agencies responsible for implementing the export control regulations: **1.** The Department of Commerce, **2.** The Department of State, **3.** The Department of Treasury.

- What is an export?
  The federal definition of an export is any item that is sent from the U.S. to a foreign destination; **1.** to anyone outside the U.S., including U.S. citizens, **2.** to foreign entities, individuals, embassies or affiliates at any location, including the U.S. "Items" include, but are not limited to, commodities, software or technology, retail software packages and technical information.

- Who is a Foreign National/Person?
  The federal definition of a foreign national is a person who is **not**: **1.** granted permanent U.S. residence, as demonstrated by the issuance of a permanent residence card, i.e., a "Green Card", **2.** granted U.S. citizenship, **3.** granted status as a "protected person" under 8 U.S.C. 1324b(a)(3), e.g., political refugees, political asylum holders, etc. This includes all persons in the U.S. as students, businesspeople, scholars, researchers, technical experts, etc.

- What is a re-export?
  The federal definition of a re-export is the shipment or transmission of an item subject to regulation from one foreign country (i.e., a country other than the U.S.) to another foreign country. Shipment or transmission may occur in any of the following ways: phone, e-mail, lab tours, meetings, and computer data. A re-export also occurs when there is a "release" of technology or software (source code) subject to regulation in one foreign country to a national of another foreign country.

- What is a deemed export?
  The federal definition of a deemed export is an export of technology or source code (except encryption source code) that is "deemed" to take place when it is released to a foreign national within the U.S. A "deemed" export situation can occur by access/use in research or training, visual inspection, or an oral exchange of information.