Technology Control Plan (TCP)

Kansas State University (K-State) is committed to export control compliance. All K-State employees and students are responsible for the export control implications of their work. They must be aware of, and must ensure that their activities conform to, export control laws and regulations. Non-compliance carries severe institutional and individual consequences, including the loss of research funding, loss of export privileges, and/or criminal and civil penalties.

This project/activity involves or has the potential to involve the receipt and/or use of export-controlled information, items, technology and/or software. As a result, the project/activity comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130) or the Department of Commerce's Export Administration Regulations (EAR) (15 CFR Parts 730 -774).

It is unlawful under the EAR or ITAR to send or take export-controlled items (including technical information, data, products, software, hardware, biological and chemical materials) out of the United States without proper authorization. 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, items, technology, or software. A foreign person is a person who is not a U.S. citizen, a U.S. permanent resident or a person who is protected under the U.S. refugee and asylum status. The law makes no exceptions for foreign graduate students.

A Technology Control Plan (TCP) is essential in preventing unauthorized access and/or use of export-controlled information, items, technology, or software. This document serves as a template for the elements of a TCP and the safeguard mechanisms to protect against unauthorized access or use. In some cases, additional security measures and safeguards may be necessary depending on specific circumstances. Contact the University Research Compliance Office (URCO) at 785-532-3224 or comply@k-state.edu for assistance in completing this form.

Steps for establishing a Technology Control Plan:

- **Step 1**: The Principal Investigator or Responsible Individual (PI/RI) develops a TCP in coordination with the University Research Compliance Office (URCO). URCO will conduct restricted party screening of all proposed participants and advise the PI/RI as necessary.
- **Step 2**: PI/RI seeks the approval of the plan by the department head and the URCO.
- **Step 3**: PI/RI reviews the TCP with all participants who will access export-controlled information, items, technology, or software. All participants must clearly be identified in the TCP. Each participant must execute the *Technology Control Plan Briefing and Certification*[1]. The PI/RI will submit all signed documents (TCP and Briefing and Certification) to URCO and retain a copy in their file.
- **Step 4**: PI/RI must periodically review the TCP as per the Self Evaluation Program stipulated in this TCP. It is the responsibility of the PI/RI to notify URCO of any anticipated changes to the TCP (e.g., personnel, scope of work, safeguards, etc.).
- **Step 5**: Record keeping – all records relating to the TCP must be retained for at least five (5) years from the date this TCP is no longer necessary to protect the information. Records will be maintained in accordance with K-State record retention policy , and 15 C.F.R., Part 762 (EAR); 22 C.F.R. §§122.5, 123.22, and 123.26 (ITAR); and 31 C.F.R. §501.601 (OFAC).

[1] Technology Control Briefing and Certification is attached to this template.

Technology Control Plan (TCP)

Title of Sponsored Project/Activity:

Principal Investigator/Responsible Individual (PI/RI): _____

Work Address: _____

Phone: _____ E-mail: _____

---

1. Describe project, activity or equipment subject to TCP:

Identified Export Controls Classification Number (ECCN) or ITAR Category if known or applicable:

Reason(s) for Control:

2. **Briefing Requirement:** The Principal Investigator/Responsible Individual is required to brief all participants on the requirements of this TCP.

3. **Authorized Personnel:** Clearly identify every person who may have authorized access to the controlled information, item, technology, or software by giving their full legal name and citizenship(s). Attach additional sheets if necessary.

Full name	Citizenship(s)	Date of Export Control Training

4. Any change in personnel will require an amendment of this TCP as described in section 8. On departure of any of the Authorized Personnel listed above, the Responsible Individual must implement appropriate measures to secure the subject matter of the TCP, including promptly collecting all keys and updating access controls.

5. **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")*

    a. Location (describe the physical location of **<u>each</u>** sensitive technology /item to include building and room numbers. A schematic of the immediate location is highly recommended):

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

c. Item Marking (Export controlled information must be clearly identified and marked as such)

d. Item Storage: Explain how the item will be secured. Soft and hard copy data, notebooks, reports and research materials must be secured by, for example, storing in locked cabinets in rooms with key-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing "export-controlled" technology must be physically secured from unauthorized access

6. **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) or stand-alone computer as appropriate, 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).

a. Structure of IT security: Describe the information technology 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.

c. 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.:

d. 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:

7. Personnel Screening Procedures

   All personnel who may have access to export-controlled items, information and/or technology must be listed on the TCP as Authorized Personnel and undergo Restricted Party Screening using export control screening software licensed by K-State. Screening Results will be maintained as part of this TCP.

8. Amendment to the TCP: Any changes to the approved TCP, including personnel changes, must be made in writing and approved by the URCO.

9. Training/Awareness Program
   All Authorized Personnel listed on a TCP must complete export control training, *Introduction to Export Compliance*, available on www.CITIProgram.org. Training is required every three years. In addition PI/RI must brief participating personnel as to the provisions of this TCP before they sign the Certification for Safeguarding Export Controlled Technology, Information or Items. If additional training is desired, please contact URCO at comply@k-state.edu

10. Self-Evaluation Program

    a. Self-Evaluation Schedule: It is recommended that the TCP be reviewed/evaluated at least once every year. Describe how often you plan to review / evaluate your TCP :

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

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

The PI/RI will submit a report on the findings of the self-evaluation to URCO via email on comply@k-stake.edu promptly.

11. Monitoring and evaluation by URCO
URCO will conduct periodic monitoring and evaluation of activities covered by this TCP and make a report. URCO will provide the PI/RI and the department/unit head with a copy of the monitoring and evaluation report, for information and action as appropriate.

12. Certification by Principal Investigator/Responsible Individual

By signing this TCP, I certify that I have read and understand all clauses found in this TCP. I certify that all information found in this TCP is accurate and complete to the best of my knowledge.

Principal Investigator / Responsible Individual

_____ _____ _____
Signature Date: Printed Name

Department/Unit Head

_____ _____ _____
Signature Date: Printed Name

University Research Compliance Office Approval

_____ _____ _____
Signature Date: Printed Name

Title: Associate Vice President for Research Compliance

Technology Control Plan Briefing and Certification
Handling of Export-Controlled Information, Items, Technology and Software

BACKGROUND

The subject matter of the Technology Control Plan (TCP) identified below may involve the use of export-controlled information, technology, items or software. The International Traffic in Arms Regulations (ITAR), enforced by the Department of State, and the Export Administration Regulations (EAR), enforced by the Department of Commerce, prohibit sending or taking export-controlled information, items, technology or software out of the U.S. and disclosing or transferring export-controlled information to a Foreign Person inside or outside the U.S. Verbal and visual disclosures are equally prohibited.

A Foreign Person is defined as any person who is not a U.S. citizen or legal permanent resident of the U.S. There are no exceptions for foreign graduate students or visiting scholars.

Generally, export-controlled means that the information, item, technology, and/or software related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use items with a capacity for substantial military application utility requires an export license, or license exception, before it may be physically exported or discussed or disclosed to a Foreign Person. Export-controlled information does not include basic marketing information about function or purpose, general system descriptions, or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain. It does not matter whether the actual intended use of export-controlled information is military or civil in nature.

PARTICIPANTS RESPONSIBILITIES

Participants may be held personally liable for violations of the EAR and the ITAR, with significant financial and criminal penalties as a result. It is extremely important that participants exercise care and caution in using, disclosing or transferring export-controlled information, items, technology, or software with others inside and outside the U.S. Export controlled information, items, technology, and/or software cannot be transferred without prior authorization from the appropriate federal agency. For example, participants must know who among proposed research project personnel and collaborators is authorized under the TCP to have access to technology-controlled information, items, technology, and/or software. Participants must secure access to export-controlled information, items, technology, or software to prevent unauthorized access or use. They must clearly identify export-controlled information, items, technology, or software. Participants must securely store export-controlled information in locked filing cabinets, locked drawers, or under password-protected computer files. Participants shall avoid moving export-controlled information from one location to another, if at all possible.

CRIMINAL/CIVIL LIABILITY AND PENALTIES

The penalty for unlawful export and disclosure of export-controlled information under the ITAR is up to two (2) years imprisonment and/or a fine of one hundred thousand dollars ($100,000). The penalty for unlawful export and disclosure of information controlled under the EAR is the greater of either a fine of up to one million dollars ($1,000,000) or five (5) times the value of the exports for a corporation and imprisonment of up to ten (10) years and/or a fine of up to two hundred fifty thousand dollars ($250,000) for an individual. *It is very important to remember that individuals may be held personally liable for export control violations even when performing a project that is funded through the University.*

Principal Investigator/Responsible Individual: _____

Department: _____

Sponsor Name: _____

Project Title/Activity: _____

Proposal/Agreement Number: _____

CERTIFICATION

- I hereby certify that I have read and understand the *Technology Control Plan Briefing and Certification on the Handling of Export-Controlled Information, Items, Technology and Software*. I understand that I could be held personally liable if I unlawfully allow access to or disclose, regardless of form or format, export-controlled information, items, technology, or software to unauthorized persons.

- I understand that the law makes no specific exceptions for non-US students, visitors, staff, postdocs or any other person not pre-authorized under a TCP to access export controlled information, items, technology or software.

- I also acknowledge that I have read the Technology Control Plan for this project/activity and have been briefed by my supervisor or by the Principal Investigator/Responsible Individual and that I agree to comply with the requirements in the TCP.

- I have taken the required export control training *Introduction to Export Compliance*, available at www.CITIProgram.org. I agree to immediately contact the Principal Investigator/Responsible Individual or University Research Compliance Office (URCO) at comply@k-state.edu with any questions I may have regarding the designation, protection, or use of export-controlled information, technology, software, or items.

Participant Name (Print): _____

Signature: _____ Date: _____

*Print and execute this **CERTIFICATION** for each person who will have access to the export controlled subject matter.