Southern Illinois University System

EXPORT CONTROLS PROCEDURES

Title: Technology Control Plans		
Procedure #: EC006	**Effective Date:** 11/01/2021	**Author:** Todd Wakeland

Purpose/Definitions: SIU may be in possession of items that are subject to U.S. export control laws and regulations. SIU aims to engage foreign nationals and host international visitors in the most welcoming manner possible, while still maintaining compliance with U.S. laws and regulations governing the export of certain equipment and materials, as well as protecting sensitive data.

Federal laws and regulations, including, but not limited to, the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) regulate the transfers of physical items, technical information, data, products, software, hardware, biological materials, or chemical materials, hereafter referred to as "*export-controlled items and information*", to certain non-U.S. persons and entities. It is unlawful under the EAR or ITAR to send or take *export-controlled items and information* 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 items and information.* 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 does not make exceptions for foreign graduate students.

In order to follow best practices, SIU shall implement a Technology Control Plan (TCP) whenever a research activity is subject to export controls. The purpose of the TCP is to help ensure compliance with U.S. export control laws and regulations, to appropriately secure the *export-controlled items and information* from unauthorized access, and ensure the research teams understand their compliance obligations and responsibilities.

The Exports Control Office shall assist the Principal Investigator (PI) of the project to develop and implement the TCP. Before any individual may have access to *export-controlled items or information*, he or she must be informed of the conditions of the TCP and agree to comply

with the security measures outlined in the TCP. SIU personnel subject to a TCP must complete an initial in-person export control training when the TCP is implemented and are required to complete follow up training annually. In addition, the Export Controls Office shall monitor compliance with the TCP and confirm its accuracy on an annual basis with the PI. It is the PI's responsibility to contact the Export Controls Office if any changes need to be made to the TCP during the course of the year.

Procedure:

NOTE: If EAR equipment is identified, but there are no additional *export-controlled items and information*, a comprehensive TCP as outlined below is not necessary. However, in order to ensure compliance with EAR requirements, an EAR Equipment Acknowledgement Form shall be completed by all parties that will be using the equipment.

Export Controls staff shall place an "SIU Export Control Property" sticker on all export-controlled equipment, whether EAR or ITAR controlled. This sticker will have a unique number on it and will be tracked on an inventory listing maintained by the Export Controls Office.

1. **Technology Control Plan Development:** When a PI or other involved party believes a TCP may be necessary, they shall contact the Export Controls Office. If the Export Controls Office determines that a TCP is needed, the Export Controls Office shall assist the PI to develop and implement a TCP to secure the *export-controlled items and information* from unauthorized access. The TCP shall be customized dependent on the security measures needed for the circumstances and situations.

   However, at a minimum, the TCP shall include the following elements:

   - A commitment to export control compliance
   - Identification of the applicable export controls and items or technologies subject to the controls
   - A description of the agreed upon physical and information security measures to control the item/technology, including as appropriate: laboratory compartmentalization, time blocking, marking, locked storage, electronic security, and/or confidential communications
   - Identification and nationality of each individual who will have access to the controlled item or technology
   - Personnel screening measures for granting access to the controlled item/technology
   - Training and awareness program – Authorized project personnel shall complete an initial export control training, along with annual follow up training.

- Self-evaluation program – An internal assessment process shall be used to review procedures, ensure all information in the TCP is current, and report findings to the Director of Export Controls on at least an annual basis.
- Appropriate security measures for disposal of the item/technology when use is complete

To aid in compliance with best practice guidance, the Export Controls Office has developed a TCP template to guide the development process. The use of the template is not required, but all elements listed above must be included in a TCP, even if the template is not used.

Following are the details for completing each section of the TCP template:

- Statement of Institutional Commitment
  - Fill in Responsible Person and Unit. The Responsible Person should generally be the PI, unless otherwise approved by the Export Controls Office.
- Program Information
  - Fill in all fields for the project related to the *export-controlled items and information.*
- Personnel Screening and Training/Awareness
  - List in the information for all project personnel as it related to the *export-controlled items and information.*
  - The Export Controls Office shall complete Restricted Party Screening for each individual and indicate the date such screening was completed.
- Export-Controlled Items and Information
  - Fill in the details for all *export-controlled items and information.*
- Physical Security Plan
  - Fill in the information related to location, storage, physical marking, and physical security measures.
- Information Security Plan
  - Coordinate with campus IT personnel as needed and fill in the information related to location, storage, access, digital marking, and security measures.
- Recordkeeping
  - Make note and ensure understanding of all recordkeeping guidance.
- Self-Evaluation
  - Fill in the Self-Evaluation Schedule.
- Termination of Export-Controlled Activity/Project
  - Fill in the Destruction of Materials section to define how the *export-controlled items and information* will be handled at the end of the research project.

2. **Unit/Export Control Approval and Responsible Person Certification:** Once the TCP has been developed, the PI's Unit Head and a member of the Export Controls staff shall approve the TCP. The PI/Responsible Person shall then certify the accuracy and their understanding of the TCP.

   If using the TCP template, the Unit Head and Export Control staff member shall sign off indicating approval of the document in Appendix A. The PI shall then sign their certification of the TCP, also in Appendix A.

3. **Participant Briefing and Certification:** The PI shall provide a briefing to all project personnel, who shall certify their understanding.

   If using the TCP template, all project personnel shall sign the certification in Appendix B.

4. **TCP Implementation:** It is the responsibility of the Responsible Person identified in the TCP to implement the security measures defined within the TCP. This includes diligence in overseeing employees so that they understand and follow the security measures and processes to be implemented. The TCP is to be a living document. The Responsible Person is responsible for conveying any changes to the Export Controls Office and updating the TCP accordingly.

5. **Recordkeeping and Termination of Export-Controlled Activity/Project:** SIU's policy is to maintain export-related records based on individual controlled items or activities. Unless otherwise provided for or instructed by the Office of the General Counsel, all records shall be maintained consistent with the SIU record retention policy, and shall be retained no less than 5 years after the TCP termination date or license termination date, whichever is later.

   Upon completion of the project, all *export-controlled items and information* must be disposed of in accordance with applicable sponsor terms and U.S. export control requirements. It may be necessary to keep certain security measures in effect after the conclusion of a research activity to comply with export control laws and regulations and protect residual export-controlled technical data, information, or equipment.

   The TCP can be closed if the export-controlled data or equipment has been returned to the sponsor, destroyed, or determined to be no longer export-controlled. However, all records and documents that pertain to export licenses and agreements related to controlled articles and technical must be retained in accordance with SIU policy and federal regulations.

Details for recordkeeping and termination of the specific export-controlled project shall be defined in the TCP. The Responsible Person is responsible for adhering to these details.