LEHIGH UNIVERSITY	**SOP: Developing a Technology Control Plan** **Responsible Office: Research Integrity**			
	ORIGINALLY ISSUED	REVISED	AUTHOR	PAGE
	17-Aug-2022	n/a	N. Coll	1 of 7

I. Purpose

This SOP outlines the process for Principal Investigator (PI) development and Export Control Officer (ECO) review of Technology Control Plans (TCPs).

II. Scope

TCPs outline the procedures and infrastructure in place to keep controlled information, technology, or equipment from being shared without proper authorization. TCPs help research groups understand what needs to be protected, and how. TCPs serve as certification to sponsors and the university that the PI is providing appropriate security for controlled information and items. PIs must submit completed TCPs for review and approval by the ECO. TCPs must be approved and fully executed prior to the commencement of the proposed activities.

Common reasons for control include, but are not limited to, the following:

- Owning and operating and/or developing restricted equipment.
  - Examples: advanced lasers, unmanned aerial vehicles (UAVs), space-related equipment, military end-use items.
- Receiving controlled information or items from a sponsor.
  - Examples: Controlled Unclassified Information (CUI), proprietary or sensitive export-restricted specifications or parameters, controlled equipment or materials.
- Restrictions within a contract.
  - Examples: publication restrictions, nationality restrictions, DFARS and some contract clauses related to security and data sharing.
- Producing restricted research results or technology, information, materials, or equipment.
  - Examples: developing or fabricating restricted items, increasing pathogenicity of select agents or certain pathogens, developing restricted software or data.

III. Relevant University Policy

Policy: Export Control

IV. Procedure

1. Identify the need for a TCP

The need for a TCP can be identified by the PI or by the Office of Research Integrity (via the ECO or designee) when initiated via other processes such as sponsored program award acceptance or purchase of export-controlled items. When they are determined to be required, TCPs must be developed, reviewed, approved, and fully executed prior to commencement of the proposed activity.

2. Draft a TCP using the TCP template.

The TCP template includes the following specific sections:

a. General Lab Information

   i. General Research Focus

   This does not need to be specific to any sponsors or funding. It should provide a brief, general overview of the PI's research focus. Consider this a blurb that could be posted on the lab's website.

   ii. Technology Control Plan Type

   The default for this section is "Lab" because most researchers who work in an area that includes restricted technology or items may have more than one project subject to export control. Some researchers will instead complete a TCP for only a single piece of equipment or a specific research team member or visitor. Choose "Lab" if unsure. The ECO will verify the TCP type prior to approving the plan.

   iii. Export Control Jurisdiction

   Options include:

   1. Unknown by PI
   2. ITAR: International Traffic in Arms Regulations
   3. EAR: Export Administration Regulations
   4. OFAC: Office of Foreign Asset Controls
   5. Other: International Treaties, Controlled Unclassified Information Categories, etc.
   6. Multiple: regulated by more than one agency or regulation, or unknown.

   The default for this section is "Unknown by PI". Some PIs may already know that most of their research falls under a certain jurisdiction. The ECO will verify this prior to approving the plan. If known, choose the appropriate jurisdiction. If unknown, choose "Unknown by PI".

b. General Lab Physical Security

   i. Building Location of Controlled Projects/Information

   This may be the same information as listed in the "General Lab Information" section above, depending on the extent to which the lab is centralized.

   ii. Building Contact

   Determine the staff person responsible for the subject building's physical security. If there is not a staff person with these responsibilities, include the PI.

   iii. Physical Location

   When possible, a floorplan of the building where the lab is located should be included as an appendix to the TCP. PIs must request building floor plans directly from Facilities for inclusion in the TCP by contacting Tara Spagnoletti (trs217@lehigh.edu).

iv. Physical Security
Describe the lab's security measures. This is especially important when lab spaces are shared with other research groups, and when equipment is stored or research is done in open areas. Examples of security measures include:

- Lab compartmentalization: cordoning off sections of labs to prevent physical or visual access on an ongoing basis or during research conduct.
- Time blocking: limiting conduct of research or use of equipment to secure time blocks.
- Marking: physically identifying export-controlled information.
- Access controls: monitoring of physical access to facilities.
- Personnel identification: requiring individuals working on research or using equipment to wear physical identification confirming their ability to access the facilities or equipment, such as a badge or card.
- Locked storage: equipment, operating manuals, lab notebooks, reports, data, and other physical documents may be stored in card swipe facilities, keyed cabinets, etc.

v. Conversations
Describe how sensitive information will be protected through verbal conversations. Examples of protections include using conference rooms or enclosed lab spaces for meetings, requiring that research project discussions are limited to identified, authorized project participants only in private areas and when other individuals are not present. Remote communication methods, such as Zoom, can be addressed in this section.

General laboratory meetings may not include discussion of sensitive or protected information subject to the TCP.

Example: "Restricted conversations will take place in [room number] and be limited to personnel who are covered under this TCP. If lab meetings take place over Zoom, they will be on a secured network."

c. General Information Technology Security

Information received, created, stored and transmitted during the conduct of an export-controlled research project will generally be considered "Level II Data" as defined by the Lehigh University Information Security Policy. Under this definition, the information should not be publicly accessible, and should be protected by relevant security controls, so that confidentiality and integrity of data is maintained.

The section of the TCP will include the following:

- i. Data Storage
  1. Address the location and technology involved in project data storage. If storage is local to Lehigh University, describe how access is controlled (e.g., a departmental shared drive accessible only to project team members). If storage is cloud-based, identify the vendor and how security features are set.
- ii. Portable Devices
  1. Describe portable computing devices used in the lab, who owns them, who has access, and whether restricted data will be stored on portable devices. If restricted data will be stored on portable devices, describe procedures used to ensure portable devices are secured.
- iii. Physical Systems
  1. Provide a basic answer. E.g., “screens are locked when computers used to access/process controlled information are not in use by authorized personnel”.
- iv. Encryption
  1. If encryption outside of standard Lehigh University encryption is commonly used, describe here. Otherwise, answer “N/A”.
- v. HPC use
  1. If HPC is being used, describe the controls or restrictions developed in collaboration with LTS.
- vi. LTS Contact
  1. List the department’s LTS professional that is contacted in the case of a computing issue.

d. Equipment List

Ultimately, all export-controlled equipment in the lab should be listed. In the beginning stages of establishing a TCP, this section may remain blank. The Office of Research Integrity will work with the PI and the Capital Asset Accounting team to evaluate and properly tag equipment. If applicable, list the individual in the department or on the research team responsible for equipment purchases and maintenance. If not applicable, leave this section blank.

Once identified, restricted items will be labeled with the appropriate Restricted Use / Export Controlled tag by the Capital Asset Management team. If the equipment is not yet appropriately tagged, note that in the CAM Tag# column.

e. Acknowledgement of Responsibilities and Signatures

Acknowledgement of responsibilities are affirmed with signatures and required by the PI, the University's Chief Security Officer, the PI's Department Chair, or the Associate Dean for Research of the requisite College if the PI is the Department Chair, and the ECO.

f. Specific Project Addendum

The addendum is specific to a sponsored program, piece of equipment, software package, technology, or international visitor. The addendum is in addition to the general lab information and is more specific and applied. When the PI does not have answers to regulatory requirement questions (i.e., 4 and 6), they should be left blank and the ECO can complete during the review process.

i. General Project Information: this section should be completed by the PI, in order for the ECO to construct the appropriate technology control plan language.
    1. Project title and/or working title
    2. Sponsor, including prime sponsor if applicable
    3. Project Start/End Date
    4. Export control jurisdiction: The default for this section is "Lab" because most researchers who work in an area that includes restricted technology or items may have more than one project subject to export control. Some researchers will instead complete a TCP for only a single piece of equipment or a specific research team member or visitor. Choose "Lab" if unsure. The ECO will verify the TCP type prior to approving the plan.
    5. Principal Investigator
    6. TCP type: The default for this section is "Lab" because most researchers who work in an area that includes restricted technology or items may have more than one project subject to export control. Some researchers will instead complete a TCP for only a single piece of equipment or a specific research team member or visitor. Choose "Lab" if unsure. The ECO will verify the TCP type prior to approving the plan.
    7. Any/all identifying numbers, e.g., LU proposal/award number.
    8. If relevant, attach proposal documents such as the Scope of Work or Deliverables/Outcomes or award documents such as proposed contracts.
    9. Description of the project: include enough detail to identify key reasons for control. For example, Department of Defense research on or with a dual-use civilian and military item. This section may look similar to the Scope of Work.
    10. Subcontracts: identify whether or not the work involves a subcontractor, or plans to subcontract out to another entity.
    11. If applicable, provide details regarding the methods planned for securely sharing controlled information.

12. Publications: describe the intended dissemination and publication plans, including the extent to which data will be shared, public presentations, etc.
13. Student theses/dissertations: export-controlled research that involves student thesis research should be coordinated via the faculty advisor/PI as early as possible to avoid any delays or disapproval for student thesis research.

ii. Specific Project Personnel: list everyone working on the project or with the equipment/technology. If citizenship details are unavailable, submit with that information omitted in order to start the review process. Depending on the reasons for control, citizenship status may ultimately be irrelevant. However, the personnel section must be completed before a final TCP is executed.

iii. Summary of Project and Control Requirements: the ECO completes this section using information provided by the PI and additional contract documents, etc. as necessary.

3. ECO review of the draft TCP

Submit the draft TCP to the ECO via email. Include all relevant attachments. The ECO will confirm receipt and will request any missing or additional information during the review process.

In review of the proposed activity and the corresponding TCP, the ECO will determine if any overlap between the specific reasons for control, personnel, and additional considerations require applying for a federal license. When the ECO determines a license is required, the ECO works with the PI directly to procure all documentation and approvals necessary to move the proposed activity forward. In these cases, the proposed activity cannot commence unless and until authorization has been obtained from the cognizant U.S. government agencies.

The review process ends when the ECO and the PI mutually agree to a final version of the TCP.

4. Circulate the TCP for execution

The TCP is circulated in DocuSign to all signatories named on the plan. The TCP template includes the following signatories, though these may be modified during the development of an individual TCP:

a. ECO
b. PI
c. Chief Information Security Officer
d. Director, Operations and Maintenance (Facilities)

e. Department Chair, or Associate Dean for Research if the PI is the Department Chair

5. Implement the TCP

The PI is responsible for overseeing timely implementation of the TCP, complying with the terms of the TCP, and ensuring that all personnel named on the TCP are aware of any subject requirements.

6. Modify or Recertify an Approved TCP

Any and all subsequent changes to an approved TCP, including the addition of new personnel, require the prior approval of the ECO. The PI is responsible for notifying the ECO promptly if conditions change such that the TCP requires modification.

The following non-exhaustive list includes changes that require a modification to the TCP:

- Significant changes to the scope of the project plan (including any new effort not originally proposed)
- Personnel additions or reassignments
- Significant IT hardware additions or deletions, or software changes
- Significant changes to physical security
- Physical moves (office or lab additions or changes)

When modifications are required, the TCP must be revised and the revised document circulated for execution by all signatories.

The PI is required to annually certify the accuracy of the TCP.

7. Terminate a TCP

The terms of the TCP remain in force as long as the technology/information is in Lehigh University's possession. Disposition of export-controlled items, equipment or information should be coordinated with the ECO. All records pertaining to the export-controlled technologies/information will be retained in accordance with Lehigh University policy and all applicable federal regulations.

8. Noncompliance with the terms of a TCP

Failure to comply with the terms of an approved TCP, including failures to modify or recertify in a timely manner, will result in revocation of approval and notification to the Department Chair, Dean, and the Vice President and Assistant Provost for Research. Failure to comply with the terms of the TCP, including but not limited to failures to modify or recertify in a timely manner, may result in denial of access to sponsored program funds for work including export-controlled items and information, denial of future funding requests by the sponsor, and may constitute a violation of U.S. export control laws, which may result in the imposition of penalties including fines and imprisonment.