**Technology Control Plan Completion Instructions:**

Principal Investigators (PIs) are responsible for developing Technology Control Plans (TCPs). TCS must be prepared following the procedure outlined in the [SOP: Developing a Technology Control Plan](https://research.cc.lehigh.edu/sites/research.cc.lehigh.edu/files/documents/ORI/SOP%20Developing%20a%20Technology%20Control%20Plan%2018-Aug-2022.pdf). Contact inexport@lehigh.edu with questions about completing and submitting a Technology Control Plan for ECO review.

|  |
| --- |
| **Section I: General Lab Information** |
| **1. Lab Name:** |            | **2. General Research Focus:** |            |
| **3. Department** |            |  |  |
| **4. Principal Investigator (PI):** |            |  |  |
| **5. Lab phone and email:** |            | **6. Lehigh University Building and Room Number:** |            |
| **7. TCP Type:** | Lab | **8. Export Control Jurisdiction:** | Unknown by PI |

|  |
| --- |
| **Section II. General Lab Physical Security** |
| 1. Location of Controlled Project / Information           | 2. Name of Building Contact:           |
| 3. Describe the physical location of sensitive technology / items / research activity, including building and room numbers.            [ ]  Check if including a floorplan of the building where the lab is located as an appendix to the TCP. |
| 4. Describe the physical security plan designed to protect the items/technology from unauthorized access. Include a detailed description of measures such as lab compartmentalization, time blocking, marking export-controlled items, personnel identification, facility access controls, and locked storage. *If there are Foreign Persons (students, faculty, staff and/or visitors) in close proximity to this controlled space, include steps taken to address the additional security factor this presents. U.S. Export Control regulations classify a Foreign Person as anyone who is not a U.S. citizen or lawful permanent resident (e.g., Green Card holder).*           |
| 5. Describe the plan for protecting export-controlled information in conversation (e.g., information conversations and more formal discussions such as lab meetings, presentations, etc.)            |

|  |
| --- |
| **Section III. General Information Technology Security** |
| 1. Describe the measures taken to protect sensitive information on IT systems within the lab. Include things like type of IS, primary users, devices, encryption, and connectivity.            |
| **Note:** all devices used for export-controlled information must be Lehigh University owned and LTS managed. Use of personally owned devices to access or store export-controlled information is not permitted. |
| 2. If portable devices are used, describe access and controls of the physical security of these items, 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. *Note*: *laptops are considered portable devices.*            |
| 3. For physical systems, describe the measures in place to prevent unauthorized viewing to these systems or equipment when processing controlled information (location, room access controls, automatic screen locking, privacy filters, screen placement, etc.).           |
| 4. If used, describe encryption:            |
| 5. If using HPC, describe the controls or restrictions developed in collaboration with LTS:       |
| 6. List the department or lab’s primary LTS professional contacted in the case of a computing issue:            |

|  |
| --- |
| **Section IV: Equipment List** |
| **Equipment Name** | **Capital Asset Management (CAM) Tag #** | **Classification Number** | **Description/Use** |
|            |            |            |            |
|            |            |            |            |
|            |            |            |            |
|            |            |            |            |
|            |            |            |            |
|            |            |            |            |
|            |            |            |            |

|  |
| --- |
| **Section V. Acknowledgement of Responsibilities and Signatures** |
| **Acknowledgement and Acceptance of the PI:**I understand my export control compliance responsibilities as the PI of this lab. I have read the Technology Control Plan (TCP) and have discussed the plan with the ECO. I understand the plan and agree to comply with all terms. I affirm that the project personnel, advisory committees, dissemination of controlled information will fit within the parameters of the referenced ECCN/ITAR categories to prevent unauthorized or unlicensed exports, reexports, or deemed exports. I agree to participate in regular audits and enhancements to this TCP. I will verify that project personnel have been briefed of their responsibilities under the TCP and have signed and acknowledged before being granted access to controlled information, material, or equipment. During the conduct of the subject project, if any question arises as to the implementation of the requirements herein, I will seek clarification from the ECO. |
| **Name:**       | **Date:**       |
| **Signature:** |
| **Acknowledgement of Chief Security Officer (CSO):**This TCP has been reviewed by a technically capable LTS security professional to ensure that any applicable regulatory or other IT security requirements can be reasonably implemented and that apparent security concerns have been addressed.  |
| **Name:**       | **Date:**       |
| **Signature:** |
| **Acknowledgement of the Director, Operations and Maintenance (Facilities):**This TCP has been reviewed and the plans for proposed physical security measures are feasible to execute given the available facilities.  |
| **Name:**  | **Date:**  |
| **Signature:**  |
| **Acknowledgement of Department Chair (or Associate Dean for Research if the PI is the Department Chair):**I acknowledge that the subject lab within my department is subject to this TCP outlining controls required by federal regulations and Lehigh University policy. If I become aware of a breach or violation of this TCP, I will inform the ECO immediately.  |
| **Name:**            | **Date:**            |
| **Signature:** |
| **ECO Acceptance:**I will ensure that the PI and project personnel are briefed of their responsibilities under this TCP. |
| **Name:**            | **Date:**            |
| **Signature:** |

|  |
| --- |
| **Specific Project Addendum****Section I: General Project Information** |
| The answers and information listed within the TCP and this addendum should be accurate and complete at the time of TCP execution and subsequent implementation. In the event of any of the following, promptly contact the ECO to modify the plan:* 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 location moves (office or lab additions or changes)
 |
| 1. Project Title: |            | 2. Sponsor (& prime sponsor, if applicable): |            |
| Working/reference title (if applicable): |            |
| 3. Project Period: | Start date:            | 4. PI: |       |
| End date:           |
| 5. LU proposal/award number: |            | 6. List any proposal/award documents (e.g., Scope of work, Deliverables/Outcomes) attached for reference. |            |
| 7. Provide a brief description of the project:            |
| 8. Will there be subcontracts under this project?:  | Yes: [ ]  | No: [ ]  |
| 9. If controlled information will be shared (sent or received) electronically, describe the secure method that will be used (e.g., encrypted email, CD, sponsor provided secure file sharing system, etc.):       |
| 10. Are publications expected to be generated from this project? | Yes: [ ]  | No: [ ]  |
| 11. Will students generate a thesis or dissertation from this export-controlled data? *Note: when export controlled research involves student thesis research, the faculty advisor/PI should coordinate as early as possible to avoid any delays or disapproval for student thesis research.* | Yes: [ ]  | No: [ ]  |

|  |
| --- |
| **Specific Project Addendum****Section II. Project Personnel** |
| Identify every person who will require authorized access to the controlled technology / item and list their citizenship/permanent residency status. * Access to controlled information should be limited to individuals who have a legitimate need to know, who have been briefed on the specifics of this TCP, and have signed in acknowledgement below.
* The PI should ask the citizenship / permanent residency status question of each individual. Research team members may be asked to provide citizenship documentation before being granted access to controlled information.
* Data security briefings are required if there are any NIST or contract-based standards on IT (see item 5 in the Summary of Project and Control Requirements below). Indicate N/A if not applicable.
 |
| **Full Name** | **Department** | **Role****(student, post-doc, etc.)** | **Country of citizenship or permanent residency** | **Date of data security briefing / training** | **Signature** |
|            |            |            |            |            |       |
|            |            |            |            |            |       |
|            |            |            |            |            |       |
|            |            |            |            |            |       |
|            |            |            |            |            |       |
|            |            |            |            |            |       |
|            |            |            |            |            |       |

|  |
| --- |
| **Specific Project Addendum****Section III. Summary of Project and Control Requirements** |
| *This section is completed by the ECO and verified by the PI prior to execution of a final TCP.* |
| **1. Reason for the TCP (e.g., access, publication restriction, etc.):**       |
| **2. ECCN/USML Category (list the ECCN or ITAR Category):**       |
| **3. Summary of any citizenship restrictions:**       |
| **4. Do non-U.S. Persons need to be preapproved by the sponsor?:**  | **Yes:** **[ ]**  | **No:** **[ ]**  |
| **5. Are there NIST or contract-based standards on IT?***(If Yes, data security training is required in addition to export control training, and should be indicated as such in the Project Specific Personnel Section of the TCP)* | **Yes:** **[ ]**  | **No:** **[ ]**  |
|  |
| **6. Check the information, material, and/or equipment subject to the controls set forth in this TCP (check all that apply):** | **[ ]**  | **Items / equipment / Software***Description:*            |
| **[ ]**  | **Technical data received from an external source (sponsor, collaborator, etc.)** |
| **[ ]**  | **Technical Data generated by the Lehigh University research team** |
| **[ ]**  | **Materials (e.g., energetic materials, fuel, carbon nanotubes, etc.)***Description:*            |
| **[ ]**  | **Items that will leave the U.S.** |
| **[ ]**  | **Other***Description:*            |
| **7. If a license or exemption is being utilized, outline the details. List any additional information needed to complete the TCP (e.g. personnel, student thesis, IT, etc.).**           |
| **8. Does the contract include specific guidance for publication restriction or approval?** | **No:** **[ ]**  | **Yes:** **[ ]** *Description:*            |