Technology Control Plan Template

**PI(s):**

**Department:**

**Phone:       Email:**

**Title of Project/Activity:**

This Technology Control Plan does not cover any materials classified higher than "Controlled Unclassified Information".

**Technical Description of Export Controlled Material(s) to Be Received and/or Used:**

**Project Personnel & Citizenship:**

**Predetermined Export Classification: ECCN:       or ITAR Category:**

**Date:**

Project Personnel

1. The PI is responsible for identifying all persons who may have access to ITAR/EAR restricted documentation and software, and that such controlled Technical Data will not be further disclosed, exported, or transferred in any manner not authorized under ITAR/EAR except with the prior written approval of the U.S. Department of State or the U.S. Department of Commerce, respectively.
2. UL Lafayette’s Office of Human Resources is responsible for confirming the citizenship status of each Project Personnel granted access to the materials by the PI(s).
3. Screening Results of all Project Personnel Clear? Yes       No

Training

1. Each Project Personnel is required to complete the University of Louisiana at Lafayette online export control training, including any additional modules pertaining to their type of project.
2. Each Project Personnel is required to attend a workshop offered by the Office of Research Integrity where any questions arising out of the online training will be addressed.
3. Date Training Scheduled:      ; Date Training Completed:      ; Completed by:
   1. Project Personnel:
   2. Project Personnel:
   3. Project Personnel:
   4. Project Personnel:

Licenses

The Office of Research Integrity and the Empowered Official must obtain licenses for any Foreign Person requiring access to an export-controlled project prior to the person receiving access to an export-controlled items or technology.

*Individuals successfully completing the steps above are considered approved Project Personnel. Individuals may not receive restricted data or hardware until they are approved.*

Facilities

1. An ITAR/EAR designated room is used for storage of all ITAR/EAR controlled physical materials (i.e., hardware, software, files, printed documentation).
2. The ITAR/EAR room is clearly marked on the exterior door (ITAR/EAR Restricted Area (ITAR projects may designate U.S. Persons only)) and this approved technology control plan is posted clearly inside the room.
3. The ITAR/EAR room is access controlled. The access process (room key or card) is managed by the PI’s department and all access requests are made in writing by the project PI. Only approved personnel will be granted access.
4. Regular custodial, recycling, and maintenance services are NOT to be provided in the ITAR/EAR room and facilities management is given instructions that staff are not to access the room unaccompanied. Project personnel are responsible for cleaning and/or escorting staff as visitors (as described below) for occasional cleaning and maintenance services.
5. The ITAR/EAR room must have a shredder or disposal container for export controlled printed matter.
6. Location (include building and room number(s), lab name, etc.):

Marking Documents and Hardware

All ITAR restricted documents and hardware are to be clearly marked with “This document contains Technical Data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.). Violations of these export laws are subject to severe criminal penalties.

Visitor and Guest Access

1. All parties entering the ITAR/EAR room who are not approved personnel must sign in and be accompanied by approved personnel. It is recommended that all visitors be approved by the PI prior to entering the facility. Foreign Persons will not be allowed to enter the access-controlled room unless all ITAR/EAR controlled materials are secured in a locked cabinet or covered.
2. Sign in sheets must include the name of the guest/visitor, a confirmation of all parties’ citizenship, a record of the responsible approved person chaperoning the visit, as well as the date of the visit.

Computer Access and Electronic Data

1. All computers that store ITAR/EAR materials must meet the minimum campus security standards. The campus minimum security standards require that the operating system is currently supported and patched, the computer is password protected and runs current virus protection software when available for the operating system, and host-based firewall is enabled to block inbound traffic. The IT Services office will validate the security of systems storing ITAR/EAR data annually. A security review can typically be conducted within one (1) business day.
2. A secure ITAR/EAR designated system is used as the primary storage for all ITAR/EAR materials. The PI or IT support personnel hired by the PI or PI’s Department is responsible for ensuring that the system is secure. The Department head shall be notified of the IP address and name of any ITAR/EAR designated system. The PI will arrange additional monitoring for the server.
3. Storage and backup of the ITAR/EAR system data is maintained in a secure facility on campus or stored on a password protected device that is clearly marked. No open remote storage of such documents is permitted (i.e., Dropbox or Google drive).
4. It is required that all ITAR/EAR data and documents be password protected. Supported data protection methods include PGP (for Windows and Mac) and TrueCrypt (for Linux). If it is not feasible to use PGP or Truecrypt, Microsoft Excel and Word 2010 or later may be used if the machine is physically secured and the password is not stored in publicly accessible location.
5. Access to UL Lafayette computers used for projects with ITAR/EAR-controlled material is managed by the PI or IT support personnel hired by the PI or PI’s Department. Only approved personnel will be granted access.
6. Remote access to these computers must use a secure connection (e.g., VPN, SSH, or similar).
7. Remotely working on ITAR/EAR restricted materials in public locations (e.g., coffee shops, airports, computer labs, etc.) is forbidden because the citizenship of onlookers cannot be verified.
8. Transfer of ITAR/EAR restricted materials to remote storage like Dropbox or Google Drive is forbidden.
9. Transfer of ITAR/EAR controlled materials to a laptop, personal computer, or portable drive (e.g., USB drive) is prohibited. If it is necessary to transfer ITAR/EAR data to such devices, a specific plan protecting the information must be clearly described, justified, approved by the ORI, and will only be granted for a specific period of time.
10. Electronic transfer of ITAR/EAR data and documents to the sponsor or approved project personnel shall use the sponsor-preferred system of delivery. All files and communication must include a statement notifying the recipient that the data is ITAR/EAR controlled. The Office of Research Integrity will provide the necessary language. A record / log of each transfer of Technical Data and date of transfer will be maintained.

Travel

1. Computers or any electronic devices, such as portable USB drives, containing ITAR/EAR data cannot leave the United States without prior approval of the Office of Research Integrity. It may be necessary to obtain an export license for such cases, which can take ninety (90) days or more.
2. Project Personnel travelling outside the United States with a laptop which may contain export-controlled materials are required to receive additional training. The Export Control Officer must be contacted thirty (30) days in advance of any anticipated international travel to ensure appropriate training. NOTE – If a license is necessary to carry the computer to the foreign country, thirty (30) days will not be enough time to obtain a license.

Destruction/Return of Materials

Destruction or Return of Materials: Describe how the export-controlled material(s) will be handled at the end of the project or when they are not needed anymore (e.g., shredding, file wipes, destroy hard drive, return to sponsor, etc.).

PI SIGNATURE:

This is to acknowledge that I have read and understand the Technology Control Plan for the stated project. I agree to update this Technology Control Plan as required and as personnel are added to or deleted from this project.

PI Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PROJECT PERSONNEL SIGNAUTRE(S):

This is to acknowledge that I have read and understand the Technology Control Plan for the stated project. I have discussed the procedures with the PI and I agree to the follow all of the procedures contained in the Technology Control Plan. If I have any questions about this Technology Control Plan, its requirements, or following any procedure, I will contact the PI for advice before proceeding.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_