**TEXAS A&M UNIVERSITY-COMMERCE OFFICE OF SPONSORED PROGRAMS**

**TECHNOLOGY CONTROL PLAN (TCP)**

 The purpose of the Technology Control Plan is to ensure compliance with federal laws or contract commitments regarding export control compliance and/or confidentiality. In general, a Technology Control Plan is a written document, signed by the person at A&M-Commerce responsible for complying with the terms in the plan and the A&M-Commerce empowered official for export control compliance, which outlines the terms upon which particular items, technical data, or technology may be kept and used on campus and/or outside the United States. The applicable laws might include, for example, the Department of State’s International Traffic in Arms Regulations (ITAR), the Department of Commerce’s Export Administration Regulations (EAR), or other legal obligation(s).

 We want this Plan to be as accurate as possible, so if there is any information you do not understand, or that is inaccurate, please contact the A&M-Commerce Empowered Official at exportcontrol@tamuc.edu.

1. **Primary Responsible Party (Principal Investigator, Person in Whose Lab or Office the Item/Technical Data will be stored/reside)**:

2. **Contact Information (Phone, Email, Physical Address on Campus) for Primary Responsible Party**:

 Primary Phone:

 Primary Email:

 Physical Address:

. (**Optional) Name and Contact Information for an Additional Administrative Contact for the Primary Responsible Party (e.g., a Business Administrator; a Secretary; etc.)**

*Please list lab manager or coordinator or other staff person who will be responsible for maintaining the technology control plan and who will serve as the contact person for questions concerning the plan if applicable.*

3. **Description of the Item, Technology or Technical Data (e.g. manufacturer notified you that equipment is controlled or you have received the data as part of a non-disclosure agreement that indicated information is export controlled):**

*For equipment, list the items including manufacturer and model number.*

*For technology (e.g. software) list the name and version of the program.*

*If you have received information as part of a non-disclosure agreement related to the effort, state who the parties to the agreement are and the general nature of the restriction (e.g. information is company proprietary and controlled under the ITAR or EAR)*

4. **Detailed description of why the Item, Technology or Technical Data is controlled (e.g. this equipment is an item controlled under the ITAR, this data or technology may not be exported from the U.S. without prior authorization)**

*Please list the reason for control. For instance, to obtain the software license, we were required to agree not to export the software. If known, please provide the applicable control number for items enumerated on the Commerce Control List.*

*Another example might be that the manufacturer provided a statement that the equipment is controlled under the ITAR and we may not export it without a license from the Department of State Directorate of Defense Trade Controls.*

5. **Security Measures, if Any: (e.g., Labeling or Other Identification of Item, Technology or Technical Data, Secure log-on access and/or encryption to maintain security of electronic files, Limited access areas, sign-in to obtain access to equipment, locked cabinets, etc.)**

*The security measures are generally project specific and will depend on what is being secured. For instance, software may be protected by not being loaded on computers that will be leaving the U.S. on international travel. Electronic technical data may be secured through encryption, password protection, or storage in non-networked locations. Paper files may be appropriately stored under lock in key (e.g. in a secured locked file cabinet in an office that is locked when unoccupied).*

*Small pieces of equipment might be stored in locked cabinets with established sign-out procedures so that a log of chain of custody is maintained. Larger equipment might require limited access facilities with an ability to track who has entered and exited.*

6. **Agreed upon list of Individual(s) authorized to access the Items, Technology or Technical Data (please notify** **exportcontrol@tamuc.edu** **as individuals needing access change):**

|  |  |  |  |
| --- | --- | --- | --- |
| Person | U.S. Citizen or permanent resident | Access/level limitations | TCP and Export Control Training Complete (Y/N) |
| *Name of Individual* | *Yes if person is U.S. citizen, green card holder or has asylum status)* | *For equipment: person will have a key and will be able to freely access, person will be able to use item under direct supervision, person will be responsible for maintenance of item, etc.* | *It is important that all individuals working with controlled items and technologies understand their specific responsibilities in maintaining the plan.* |
|  |  | *For technology and technical data: Will person be able to directly access the data, be given minimal information required to perform related fundamental research, or simply participate in discussions?* |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*The information provided here is used to screen eligibility of persons to access controlled information (i.e. to ensure that the individuals do not appear on banned parties and specially designated nationals lists). It is important that this screening occur prior to giving individuals access to export controlled items or information. Please make sure this information is kept current.*

8. **What will be done with the controlled technical data, or item at the end of the project?**

*The end of a sponsored research activity does not eliminate the obligation to safeguard export controlled equipment, technology or technical data. As a result, a technology control plan needs to remain in effect as long as the export controlled materials remain on campus. Please indicate here if the materials will be retained on campus, returned to the sponsor, or destroyed. The Research Compliance Coordinator will work with the PI to determine when controls of retained materials and information are no longer required.*

**Thank you very much** for your cooperation in implementing this Technology Control Plan. If you have any questions, please contact exportcontrol@tamuc.edu. Once the form is completed, please sign and date below, and return to exportcontrol@tamuc.edu.

**Certification**: I hereby certify that I have read and understand this Technology Control Pan and my obligations under federal law and A&M-Commerce procedures regarding the item, technology, or technical data identified in this TCP. I agree to take the actions set forth in this TCP and, if applicable, to comply with the terms of any license governing the item, technology or technical data and the terms in any contract regarding such item, technology or technical data.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[INSERT NAME OF PRIMARY RESPONSIBLE PARTY]

CC: Department Head for Responsible Faculty or Staff Member

 Dean for School of Responsible Faculty Member or Vice President of Responsible Staff Member

 Vice Provost for Research, Office of Sponsored Programs

FOR EMPOWERED OFFICIAL TRACKING PURPOSES (to be completed by Empowered Official or his/her designee):

TCP Number: [INSERT TRACKING NUMBER HERE]

EAR LICENSE NUMBER, IF APPLICABLE?

ITAR LICENSE NUMBER, IF APPLICABLE?

OFAC LICENSE NUMBER, IF APPLICABLE?

Summary of Major License and Recordkeeping Terms:

Primary Responsible Party: [INSERT NAME HERE]

Contact Information for Primary Responsible Party:

 Physical Location of Item/Technical Data for this TCP: [INSERT HERE]

 Phone Number for Primary Responsible Party: [INSERT HERE]

 Email: [INSERT HERE]