**OFFICE OF RESEARCH**

**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.

Prairie View A&M University (PVAMU) is committed to export control compliance. It is the policy of PVAMU to comply with United States export control laws and regulations. All employees and students must be aware of and are responsible for the export control implications of their work and must ensure that their activities conform to export control laws and regulations. Individuals and the university may be subject to severe penalties for violations of export control laws and regulations, including the loss of research funding, loss of export privileges, as well as criminal and civil penalties.

In general, a Technology Control Plan is a written document, signed by the person at PVAMU responsible for complying with the terms in the plan and PVAMU’s 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).

This project/activity/equipment involves or has the potential to involve the receipt and/or use of Export-Controlled Items, Technology or Information. As a result, the project/activity comes under the purview of either the State Department’s International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130) or the Department of Commerce’s Export Administration Regulations (EAR) (15 CFR §§734.8 and 734.9) and/or other export control regulations.

Export-controlled technical information, data, items, software, hardware, biologicals and chemicals must be secured from use and/or observation by unauthorized foreign nationals.

In accordance with U.S. export control laws and regulations, a Technology Control Plan (TCP) is required to prevent unauthorized access and/or use of export controlled items, information, technology or software. This document serves as a basic template for the minimum elements of a TCP and the safeguard mechanisms to protect against unauthorized access or use. Security measures and safeguards shall be appropriate to the export classification.

If there is any information you do not understand, please contact PVAMU’s Export Controls Officer at 936-261-1553 or research@pvamu.edu.

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

|  |  |
| --- | --- |
| **Name:** |       |
| **Primary Phone Number:** |       |
| **Primary Email Address:** |       |
| **Physical Address:***(location of item(s))* |       |

. (**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.*

|  |  |
| --- | --- |
| **Name:** |       |
| **Primary Phone Number:** |       |
| **Primary Email Address:** |       |
| **Physical Address:** |       |

 **Title of Project or Activity**

 *Please list the grant title(s) if applicable*

|  |  |
| --- | --- |
| **Title:** |       |

 **Description of the Export Controlled Item, Technology, Software 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.*

|  |  |  |
| --- | --- | --- |
| **Item Name:** | **Manufacturer:** | **Model Number:** |
|       |       |       |
|       |       |       |

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

|  |  |
| --- | --- |
| **Name:**  | **Version:** |
|  |  |
|  |  |

*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)*

|  |  |
| --- | --- |
| **Name:**  | **Nature of the Restriction:** |
|  |  |
|  |  |

 **Detailed description of why the Item, Technology, Software 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. This is also called the Identified Export Control Classification Number (ECCN).*

*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. If so, please provide the ITAR Category.*

|  |
| --- |
| **Description:**  |

 **Servicing of Item, if Any: (Provide a description of how this item will be serviced or repaired during its lifetime and how custodial and related services will be addresses, including disposal and destruction)**

|  |  |
| --- | --- |
| **Name of Item:** | **Description:** |
|  |  |
|  |  |

 **Security Measures, if Any: (e.g., Labeling or Other Identification of Item, Technology, Software 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.*

*Data and/or items, technology must be physically shielded in secured lab spaces to prevent observation or possession by unauthorized individuals or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of “work-in-progress items.”*

|  |
| --- |
| **Description:** |

**Agreed upon list of Individual(s) authorized to access the Items, Technology, Software or Technical Data (please notify** **research@pvamu.edu** **as individuals need access changes):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** | **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?* | *All individuals must log onto Train Traq and complete the Texas A&M University online training course # 2111873 “Export Controls – Technology Control Plans”* |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |

*The information provided above 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. Any change in personnel will require an amendment to this plan. On departure of any of the personnel described above, appropriate measures must be implemented to secure the subject matter of the TCP, including all keys and updating access controls.*

 **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, software 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 Director of Research Compliance will work with the PI to determine when controls of retained materials and information are no longer required.*

|  |
| --- |
| **Description:** |

**Thank you very much** for your cooperation in implementing this Technology Control Plan. If you have any questions, please contact the Director of Research Compliance at 936-261-1588 or research@pvamu.edu. Then, please sign and date below, and return to research@pvamu.edu

**Certification**: I hereby certify that I have read and understand this Technology Control Plan and my obligations under federal law regarding the item, technology, software or technical data identified in this TCP. I certify that all information found in this TCP is accurate and complete to the best of my knowledge. 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, software or technical data and the terms in any contract regarding such item, technology, software or technical data. I agree to brief my staff on the requirements of this TCP. I understand that any changes to the approved plan, including personnel changes and location changes, must be approved in writing.

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

NAME OF PRIMARY RESPONSIBLE PARTY

**Reviewed by:**

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

Crysta Mendes, M.A.

Associate Director of Research Compliance

Export Controls Officer

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

Cajetan Akujuobi, M.B.A., Ph.D., E.E.

Empowered Official

Vice President for Research, Innovation, and Sponsored Programs

CC: Chair of Department for Responsible Faculty Member