

Texas A&M AgriLife | Technology Control Plan

Texas A&M AgriLife is committed to export control compliance. It is the policy of AgriLife to comply with United States export control laws and regulations. All employees 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/agency 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.

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 will exhibit the safeguard mechanisms to protect against unauthorized access or use. Security measures and safeguards shall be appropriate to the export classification.

Establishing a TCP is a multi-step process. The first step is the assessment and approval phase where the principal investigator/responsible individual (PI) develops a TCP in coordination with AgriLife Ethics and Compliance and seeks approval of the plan from the PI's department/unit head, and AgriLife Ethics and Compliance. When all approvals have been secured, the PI shall review the TCP with all users, and each user will execute a copy of the briefing and certification form at the end of the TCP outlining individual responsibilities for handling export controlled technology, information, and/or items. When all users, including the PI, have executed the TCP briefing and certification, the PI submits all signed documents to AgriLife Ethics and Compliance, and retains copies for their files, and implements the TCP. AgriLife Ethics and Compliance will follow up with the PI each year to check that information has stayed the same. It is the PI's responsibility to notify AgriLife Ethics and Compliance of any anticipated changes to the TCP (e.g., personnel, scope of work, safeguards, etc.).

Title of Project or Activity:

Principal Investigator/Responsible Individual:

Identified Export Control Classification Number (ECCN) or ITAR Category: _____

Briefing Requirement | The Principal Investigator/Responsible Individual is required to brief their staff on the requirements of this TCP.

AgriLife TCP #

1. *Personnel* | On each certification page, every person, including their country of citizenship, who may have authorized access to the controlled information, technology, or item will be listed on their individual pages and must sign. Any change in personnel will require an amendment of this plan as described below in Section 5. On departure of any of the personnel described below, appropriate measures must be implemented to secure the subject matter of the TCP, including collecting all keys and updating access controls.
2. *Personnel Screening Procedures* | All persons who may have access to export-controlled items, information, and/or technology must be listed on the TCP and undergo Restricted Party Screenings. Screening results will be maintained as part of this TCP.
3. *Physical Security Plan* | 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.

Location (include building and room numbers, lab name, etc.)

Physical Security and Item Storage | Provide a description of your physical security plan designed to protect the item/technology from unauthorized access or unauthorized removal of technical information, data, items, software, hardware, biologicals, or chemicals (e.g., secure doors, limited access, security badges, locked desks or cabinets, secure computers, marking all physical items, etc.). Both soft and hard copy data, notebooks, reports, and research materials are stored in locked cabinets; preferably in rooms with key-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing "export-controlled" technologies are to be physically secured from unauthorized access.

Physical Security:

Item Storage:

Servicing of Item:

Janitorial Service:

Destruction or Return of Materials:

Information Security Plan:

Amendments:

4. *Export License Requirements*

AgriLife TCP #

5. *Amendments* | Any changes to the approved plan, including personnel changes and location changes, must be approved in writing. An amendment will be created in the office of AgriLife Ethics and Compliance and sent to the PI for review and approval.
6. *Training* | All participants listed on a TCP must complete export control online basic training (TrainTraq Course #2111212), sign the Certification for Safeguarding Export Controlled Technology, Information or Items, and be briefed by the PI/Responsible Individual as to the restrictions of this TCP. Please contact AgriLife Ethics and Compliance at 979.845.7879 to schedule additional training.
7. By signing this TCP, I certify that I have read and understand all clauses found in this TCP. I certify that all information found in this TCP is accurate and complete to the best of my knowledge.

Principal Investigator/Responsible Individual

Date

Principal Investigator/Responsible Individual

Date

Reviewed By (AgriLife Ethics and Compliance)

Date

Jennifer Green

Printed Name

AgriLife TCP #

Technology Control Plan Briefing and Certification on the Handling of Export-Controlled Information, Items, Technology, and Software

BACKGROUND | The subject matter of the Technology Control Plan (TCP) may involve the use of export-controlled information, technology, items, or software. The International Traffic in Arms Regulations (ITAR), enforced by the Department of State, and the Export Administration Regulations (EAR), enforced by the Department of Commerce, prohibit sending or taking export-controlled information, items, technology, or software out of the U.S. and disclosing or transferring export-controlled information to a Foreign Person inside or outside the U.S. Verbal and visual disclosures are equally prohibited.

Generally, export-controlled means that the information item, technology, and software related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing or use items with a capacity for substantial military application utility requires an export license, or license exception, before it may be physically exported or discussed or disclosed to a Foreign Person. Export-controlled information does not include basic marketing information about function or purpose, general system descriptions, or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain. It does not matter whether the actual intended use of export-controlled information is military or civil in nature.

PARTICIPANTS RESPONSIBILITIES | Participants may be held personally liable for violations of the EAR and the ITAR, with significant financial and criminal penalties as a result. With that in mind, it is extremely important that Participants exercise care and caution in using, disclosing, or transferring export-controlled information, items, technology, or software with others inside the U.S. and outside without prior authorization from the appropriate federal agency. If a Foreign Person is having access to export-controlled information, the State Department or the Department of Commerce (depending on whether the ITAR or the EAR controls the technology) must grant a license authorizing that person to do so. Participants must secure access to export-controlled information, items, technology, or software to prevent unauthorized access or use. They must clearly identify export-controlled information, items, technology, or software and make copies of export-controlled information only when necessary. Participants must securely store export-controlled information in locked filing cabinets, locked drawers, or under password-protected computer files. Participants should avoid moving export-controlled information from one location to another.

CRIMINAL/CIVIL LIABILITY AND PENALTIES | The penalty for unlawful export and disclosure of export-controlled information under the ITAR is up to two (2) years imprisonment and/or a fine of one hundred thousand dollars (\$100,000). The penalty for unlawful export and disclosure of information controlled under the EAR is the greater of either a fine of up to one million dollars (\$1,000,000) or five (5) times the value of the exports for a corporation and imprisonment of up to ten (10) years and/or a fine of up to two hundred fifty thousand dollars (\$250,000) for an individual. *It is very important to remember that individuals may be held personally liable for export control violations even when performing a project that is funded through AgriLife.*

AgriLife TCP #

Principal Investigator/Responsible Official

Unit

Title of Project/Activity

Technology Control Plan Number

CERTIFICATION

- I hereby certify that I have read and understand this Briefing and Certification. I understand that I could be held personally liable if I unlawfully allow access to or disclose, regardless of form or format, export-controlled information, technology, software, or items to unauthorized persons.
- I understand that the law makes no specific exceptions for non-US students, visitors, staff, postdocs, or any other person not pre-authorized under a TCP to access export-controlled information, technology, software or items.
- I also acknowledge that I have read the AgriLife Technology Control Plan for this project/activity and have discussed the plan with my supervisor (if not the PI/Responsible Individual), and that I agree to comply with the requirements in the TCP.
- Furthermore, I have taken the System's Export Control Training as set forth in the TCP, and as prescribed by AgriLife Rule 15.02.99.A(X)1 *Export Controls*. I agree to immediately contact AgriLife Ethics and Compliance at 979.845.7879, with any questions I may have regarding the designation, protection, or use of export-controlled information, technology, software, or items.

Participant Name

Citizenship

***Training Completion
Date***

Participant Signature

Date

*Print and execute this **BRIEFING and CERTIFICATION** for each person who will have access to the export controlled subject matter.

AgriLife TCP #