University Export Control Program
TECHNOLOGY CONTROL PLAN

Project Title			
PI Name		**PI Department**	
Sponsor		**Prime**	
Project Start Date		**Project End Date**	
UA Account No.		**Sponsor Award No.**	

Applicable Export Classifications	
ITAR – USML Category	
EAR – CCL ECCN	

This Technology Control Plan describes the procedures necessary to protect certain export-controlled equipment, software, materials, and technology/technical data from inadvertent transfer and access (oral, visual, electronic, physical, etc.) by unauthorized personnel, including non-U.S. persons as defined within the export regulations. These procedures include physical and information security, procurement, shipping/transporting, personnel screening, training and awareness, and compliance assessment. This plan will also be used to control the disposition of research project equipment, software, materials, and technical data when the project is terminated.

I. COMMITMENT

It is the policy of the University of Arizona to comply with all United States export control laws and regulations, including the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and the Office of Foreign Assets Control (OFAC). The University Export Control Program (UECP) is responsible for the implementation and monitoring of technology control plans as applicable. Kay Ellis, Director, University Export Control Program, is the UA Empowered Official for export controls.

The individual(s) responsible for and committed to implementing and ensuring compliance with this TCP is indicated above.

II. DESCRIPTION

(INSERT: Provide a detailed description of the scope of the project and clearly define the ITAR technical data, hardware, and/or defense services).

Research activity locations (offices, labs, buildings) are listed in ***Attachment 1*****.**

NOTE: Changes to I and II above will require an amendment to the existing TCP.

III. PHYSICAL SECURITY

University of Arizona policy requires all researchers appropriately protect export-controlled equipment, materials, software, and technology/technical data. Individuals identified within this TCP are responsible for the secure maintenance and protection of ALL export-controlled equipment, materials, software, and technology/technical data as follows:

GENERAL PROCEDURES

LOCATIONS

Export-controlled data and documentation will only be secured (locked in a drawer or cabinet) or accessed in locations (offices, labs, buildings) listed on Attachment 1**.** Determine who has access to

locations listed in Attachment 1. If a cipher lock is used, regularly change the code to avoid unauthorized access.

Due to increased risks of working with export-controlled data off-campus, work from home with export-controlled data will only occur when deemed necessary.

Notify UECP of shared office or residential spaces (if working remotely) with non-US Persons.

STORAGE
Back-up hard drives, flash drives, and documents that contain export-controlled data or information will be stored in a secure location (e.g. locked drawer or cabinet) identified in Attachment 1.
Only the persons who have signed this TCP will have access to information.

DOORS
Doors to individual offices or workspaces will be closed and **"Export Control Restricted: Unauthorized Non-U.S. Persons Not Permitted"** signs will be posted during times that export-controlled information is visible on the desk or workspace. Export-controlled data and documents will be cleared and secured in locked drawers, cabinets or cleared from screens/equipment when unattended.

SHARED SPACES
Time-blocks will be established for shared offices/lab(s) identified in Attachment 1. During that designated time, non-U.S. Persons will not be allowed access to the room. The time-block calendar will be distributed to all persons who have a key to this lab, as well as posted on the entry door to the lab.

VISITORS
LOGS must be maintained to record *physical* access by non-project personnel when ITAR/EAR information is visible on workspace, computer screen, etc.

- If the visitor is a non-UA employee, restricted party screening must be conducted prior to the visit.
- The visitor must be a U.S. Citizen or U.S. Permanent Resident if the project data is ITAR-controlled.
- If the data is EAR-controlled, a prior evaluation and approval must be conducted and given by UECP based on the CCL controls and the citizenship of the proposed visitor.
- Facilities Management is not considered a visitor; however, export controlled data should not be in view.
- Student office visits, if applicable, will not be conducted when project personnel are actively conducting research when ITAR data is visible.
- Non-U.S. persons will not be allowed access to export-controlled items unless prior government approval has been obtained in the form of a license or an exception/exemption (when applicable). The PI will work with UECP to review available licensing options in advance.

DOCUMENTS AND ITEMS
LABELING export-controlled items will occur by suitable means and shielded from unauthorized visual access when in use. UA-generated documents containing ITAR/EAR-controlled technical data shall be marked "**ITAR/EAR-controlled: Do Not Distribute to Non-U.S. Persons**."

PRINTING Use a printer in the facility and retrieve immediately. Documentation will be labeled and secured as described above.

MAIL (via USPS, UPS, FedEx) of ITAR/EAR-documents should be tracked. All documents will be marked as described above. Documents will be sealed in an inner envelope/box and marked "**ITAR-CONTROLLED** (certain EAR-controlled when applicable): **NO NON-US PERSON ACCESS**" on the outside of the inner envelope/box; i.e., no markings on the outer packaging.

HAND-CARRY TRANSPORT of items or data will remain secured and in the possession of the individual(s) listed in this TCP to prevent access by unauthorized persons when moved out of the facility.

DISPOSAL
Printed matter containing export-controlled data will be disposed of by crosscut shredding prior to disposal. The use of shred barrels located on the same floor is acceptable. Disposal of export-controlled data information on computers or portable digital media devices will be coordinated with UECP.

Disposal of export-controlled equipment will occur in coordination with UECP.

[INSERT: If there are physical security measures not described above that are needed to secure ITAR project information such as badging, escorts, visitor logs, and other types of building access restrictions, insert here.]

TRAVEL OUTSIDE THE U.S.
Travel outside the U.S. with export-controlled items or data may require prior authorization (license) from the appropriate government agency. **This includes access of export-controlled data while abroad.** UECP will provide exceptions or apply for authorizations as needed. The traveler should work with UECP to obtain such authorization well in advance of travel.

IV. INFORMATION SECURITY

University of Arizona policy requires all researchers appropriately secure certain export-controlled digital research data. Individuals identified within this TCP are responsible for the secure maintenance and protection of all export-controlled data and information. Digital export-controlled data/information will be protected as follows:

COMPUTERS & DEVICES
Desktop/Laptop computers (including flash drives and back-up hard drives) will use password protected-encrypted folders, encrypted files, or encrypted hard drives for working with and storing export-controlled data.

- **Removable storage devices used for ITAR data** will be encrypted at the file/folder level **or** at the device level with FIPS 140-2 Level 2 standard encryption.

- **All computers** that contain export-controlled information will be locked and password protected when unattended.

Digital files containing export-controlled information will be password protected and encrypted.

LABEL all devices (e.g., flash drives, laptops, computers, back-up hard drives) will be clearly labeled "**ITAR**" or "**EAR**", as appropriate.

EMAILED export-controlled data (distributed or received) **must be encrypted**, with passwords provided separately.

OFF-CAMPUS DATA ACCESS
Public wifi hotspots will not be used to access export-controlled technical data. Only UA VPN will be used in secure (not open) locations. Project work with data will not occur in public spaces.

DISPOSAL
Portable digital media devices that contain technical data will be physically destroyed (*i.e.,* rendered unusable) when the data is no longer needed to be retained. The PI shall notify UECP when such action occurs.

VIDEO CONFERENCES
When using video platforms to discuss ITAR technical data, enable security features (e.g., passwords and do not record). Zoom security - https://it.arizona.edu/documentation/zoom-security-options.

[INSERT: If additional measures not listed above are needed to ensure the project's information security, insert here]

NOTE*:* Discussions and/or meetings involving export-controlled technical data may be conducted occasionally by and with team members and/or sponsor representatives in locations other than those identified herein (conference rooms, not in hallways). Care will be taken to ensure conversations are not overheard by unauthorized non-U.S. Persons, and data will be protected as outlined in this TCP.

V. PROCUREMENT OF ITAR CONTROLLED SPECIALLY DESIGNED ITEMS OR ITAR CONTROLLED EQUIPMENT

If applicable for this project, the procurement of certain export-controlled items such as parts, tooling and equipment specifically designed, developed, configured, adapted, or modified for use with an export-controlled item must be purchased from suppliers and vendors who can certify the suppliers/vendors are compliant with U.S. export control laws and regulations.

It is the responsibility of the PI/Project Director and/or the appropriate College/Department Administrator to obtain signed *Vendor Certification* letters. The original documentation must be kept on file by the PI/Project Director and/or the appropriate College/Department Administrator and be available for review by the UECP. (The *Vendor Certification* letter can be obtained at: http://rgw.arizona.edu/compliance/export-control-program/liaison-toolbox or by directly contacting UECP.

A restricted party screening must be completed on all vendors, including those where a P-Card is utilized. The University of Arizona will not do business with a vendor on a denied list. UA's procedures for restricted party screening can be found on the UECP website at: http://rgw.arizona.edu/compliance/export-control-program/procedures-for-restricted-party-screenings.

ITAR equipment that is purchased or given to a PI must be identified in the TCP and a label attached to the item indicating that it is "ITAR-Controlled". Only individuals authorized in this TCP are allowed access to ITAR-controlled equipment or items.

Delete the above and substitute with the following, if it is applicable:
No procurement of specially designed, configured, adapted, or modified export-controlled parts, tooling, or purchase of ITAR equipment is anticipated for this project. If circumstances change, the Lead PI will contact UECP.

VI. SHIPPING/TRANSPORTING

Shipping export-controlled items outside the U.S. or to Foreign Persons **must be coordinated with the UECP**.

ITAR items *will* require a license from Department of State and cannot be shipped until the license is approved and received by UECP.

EAR-controlled items *may* require a license from the U.S. Department of Commerce and if required, cannot be shipped until the license is approved and received by UECP.

The UECP will apply for all export licenses. Copies of the license will be retained by the UECP and a copy will be sent to the PI, Project Director, or their designee. The Department Administrator, PI, or Project Director must send a copy of all shipping paperwork to the UECP.

If ITAR-controlled, only the inner packaging of the box or container will be marked **"ITAR-CONTROLLED - NO NON-U.S. PERSON ACCESS"** and will be placed inside of an unmarked box, crate or container for shipping or transporting.

Obtain from the receiver protocols for receiving export-controlled items so that the item is received by a U.S. Person (unless a license is obtained).

Consult a shipping Broker prior to shipping equipment/items internationally.

Delete the above and substitute with following, if it is applicable:
No international shipping activities are anticipated for this project. If circumstances change, the Lead PI will contact UECP in advance. Shipment may require an export license which must be obtained by UECP prior to shipment. Shipping / transporting efforts do not include hand-carrying items.

VII. PERSONNEL SCREENING

All personnel who will have access to export-controlled technology related to this research project, including IT personnel are listed in Section XI, Certification.

The Project Director or lead PI will notify UECP if personnel need to be added to or removed from this TCP. All personnel assigned to this project and all visitors who will be given access to potentially ITAR-controlled data, including visual access, will be screened against U.S. Government denied parties lists prior to being given such access. UA's procedures for restricted party screening can be found on the UECP website at: http://rgw.arizona.edu/compliance/export-control-program/procedures-for-restricted-party-screenings.

VIII. TRAINING AND AWARENESS

All project personnel are required to take a mandatory online training course, receive a briefing by UECP and certify their understanding of this TCP ***before*** they are authorized to work on the project.

Every two years a refresher training course is required for personnel included on this TCP. The UECP will confirm that all project personnel listed in Section X have completed the mandatory training requirements by the end of two calendar years of date of signature to the TCP. Failure to complete required training may affect the individual's continued access to export-controlled projects in this facility.

Information regarding export control training : http://rgw.arizona.edu/compliance/export-control-program/export-control-training.

IX. COMPLIANCE ASSESSMENT

As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process to review procedures. An internal audit should be completed by the Project Director/PI and (or) his/her designee. Any concerns should be reported to the UECP. Please see ***Attachment 2*** of this TCP for the self-audit checklist.

The UECP will conduct periodic evaluations and/or training to assess compliance with the TCP procedures. A formal audit will be conducted by the UECP annually.

Any changes to the approved procedures, locations, or personnel having access to export-controlled materials covered under this TCP will be cleared in advance by the UECP. The TCP will then be updated to accommodate changes in personnel or locations. Authorized personnel should contact the UECP (export@arizona.edu) if there are any questions or concerns related to this TCP.

X. PROJECT TERMINATION

Security measures, as deemed appropriate, will remain in effect after the project has ended to protect the export-controlled information or until the export-controlled information has been destroyed or determined to be no longer ITAR-controlled. Disposition of export-controlled equipment, software, and technical data upon project termination shall be coordinated with the UECP.

All records pertaining to the **export** of export-controlled items shall be retained for a period of five years from date of license expiration and in accordance with University policy and applicable federal regulations.

This Technology Control Plan is approved by the University of Arizona Export Control Program.

Signature by	**Date**
University Export Control Program	

XI. CERTIFICATION

I hereby certify that I have received a briefing on the U.S. export control laws and regulations and a copy of this Technology Control Plan (TCP). I have had an opportunity to ask questions and understand and agree to follow the procedures outlined in the TCP. I will report any concerns to UECP. I understand that I could be held personally liable if I unlawfully disclose export-controlled information to unauthorized non-U.S. Persons.

Name (Printed)	Citizenship	Signature	Date

Any project personnel to be added or removed from Section X, Certification, above must be coordinated with the University Export Control Program (UECP). The PI, Approval Holder, or his/her designee may contact UECP at export@arizona.edu.

ATTACHMENT 1

The University Export Control Program must be notified when there are additions or changes.

Export-controlled information covered under this TCP will be stored and (or) accessed in the following locations outlined below. Conference rooms where discussions are held are not listed.

Temporary situations requiring participants to store or access data in off-campus locations will only occur due to extraordinary circumstances. Before doing so, participants will confirm that security measures provided in this TCP can be followed in the off-campus location and report to UECP any unique considerations that may increase the risk of unauthorized access to protected information, including Foreign Persons residing in or frequenting the location.

Any suspicious activity/theft will be reported to UECP (export@arizona.edu) as soon as possible.

Storage/access will resume on campus as soon as possible.

Building / Location	Room #	Room Name	Security Method	Shared Space (Y / N)

The University Export Control Program should be notified if there are additions or deletions to the above substance(s) use or storage locations. Only Attachment 1 will be updated.

ATTACHMENT 2

TCP Internal Self Audit Checklist

Date: _____
Auditor: _____
Location: _____

Item	Description	Determination ("Y", "N", "N/A")	Note
Physical Security			
1	Door Closed		
2	Door Locked		
3	Restricted Access Sign Posted		
4	Clean Desk		
5	Export-Controlled Equip Labeled		
6	External devices Encrypted and Secured		
7	Hard Copies Locked/Labeled		
8	Visitor Logs Maintained (if applicable)		
9	PEC Secured During Transport		
10	PEC Taken Outside US		
11	Is there a License to take Outside US		
12	PEC Printed on Secure Printer		
Information Security			
13	EEC Stored in separate Encrypted Folders		
14	Data/Information Stored on Secure Server		
15	Data Transmitted Securely		
16	Any EEC Sent via E-Mail		
17	Was the E-Mail Encrypted		
18	Computer Set Up for EEC Data		
19	Desktop or Laptop Has Encrypted Files / Folders		
20	Transported EEC Secured		
21	EEC Taken Outside US		
22	Is there a License to take Outside US		
General			
23	People Not on the TCP in the Area		
23	Auditee has Current Copy of TCP		
25	Auditee has read and been briefed on TCP		
26	Auditee has signed the TCP		
27	Is there a 125.4(b)(10) Exemption		
28	If Yes, has FN signed Exemption Yearly		
29	If Yes, has Director / Lead Signed		
30	Any NDA's Associated with Project		
31	If Yes, Has the NDA been signed yearly		
32	Vendor Certification (if applicable)		
33	Shipping Paperwork (if applicable)		
34	Any Known Export of PEC/EEC		
35	Records of Export to Non-U.S. Entity		

PEC = Physical Export-Controlled Information EEC= Electronic Export-Controlled Information FN= Foreign Person