**Export Control**

**Technology Control Plan (TCP)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** |  | | |
| **Responsible Party** |  | **Date Implemented** |  |
| **College /  Department** |  | **Control Plan Type** |  |

**TABLE OF CONTENTS**

A. COMMITMENT 2

B. DESCRIPTION 2

C. PHYSICAL SECURITY 2

D. INFORMATION SECURITY 4

E. PUBLICATIONS AND PRESENTATIONS 6

F. PROCUREMENT 6

G. SHIPPING/TRANSPORTING 6

H. PERSONNEL SCREENING 7

I. TRAINING AND AWARENESS 7

J. REPORTING 7

K. COMPLIANCE ASSESSMENT 8

L. TERMINATION 8

M. CERTIFICATION 9

N. APPROVALS 9

O. INDIVIDUAL SIGNATORY PAGE 10

P. INTERNAL SELF AUDIT CHECKLIST 11

This Technology Control Plan (TCP) describes the procedures to protect certain export-controlled equipment, software, materials, technology, and technical data from transfer and access (oral, visual, electronic, physical, etc.) by unauthorized personnel, including non-U.S. Persons. These procedures include physical and information security, procurement, shipping/transporting, personnel screening, training and awareness, and compliance assessment. This TCP includes protocols to control the disposition of research project equipment, software, materials, and technical data.

# COMMITMENT

It is University of Arizona policy 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). Export Control is responsible for the implementation and monitoring of TCPs. The Director of Export Control is the University’s primary [Empowered Official](https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.67).

# DESCRIPTION

The protocols described in this TCP apply to the items listed below that are specific to this Control Plan:

* Projects
* Agreements (NDAs, proposals)
* Data
* Equipment
* TCP Personnel
* Research activity locations (offices, labs, buildings, chemical storage)
* Licenses and exceptions

Specific items are documented in the Agiloft Data Management System (Agiloft) where they can be viewed by authorized individuals.

Please communicate any changes to Export Control ([export@arizona.edu](mailto:export@arizona.edu)).

# PHYSICAL SECURITY

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

## LOCATIONS

Provide Export Control with the names of individuals who have access to research activity locations specific to this TCP.

Regularly change cipher codes, key, and card accesses to avoid unauthorized access.

**NOTE:** Take precautions to prevent unauthorized persons from overhearing discussions and/or meetings involving export-controlled data.

## WORKSPACES

* Close doors and post **“Export Control Restricted: Unauthorized Non-U.S. Persons Not Permitted”** signs when export-controlled information and ITAR items are visible. ([download sign](https://research.arizona.edu/sites/default/files/2025-01/Sign_EC-Restricted-Access-2016Nov4.pdf)).
* **Secure** data, documents, and hard/flash drives in locked drawers or cabinets. **Only the individuals who sign this TCP may have access.**
* **Do not permit unauthorized non-U.S. Persons** entry when export-controlled information is visible without Export Control authorization.

## SHARED SPACES

**Establish time-blocks** for shared locations with non-U.S. Persons who are not authorized to access export-controlled data related to this TCP/project. During that designated time, unauthorized non-U.S. Persons cannot access the room. Distribute the time-block calendar to all persons who have access and post in the room.

## VISITORS

When visitors enter a workspace where export-controlled information is visible (computer screen, white-board, desktop, etc.):

* Confirm visitors are U.S. persons prior to allowing entry.
* Conduct [Restricted Party Screening](https://research.arizona.edu/compliance/export-control-program/procedures-for-restricted-party-screenings) (RPS) on non-UA visitors prior to allowing entry.
* Use and maintain [visitor logs](https://research.arizona.edu/compliance-public/export-control-program/liaison-toolbox-forms) to record *physical* access by non-project personnel.
* Project personnel will escort visitors.

## LABELS

* **Request that all sponsor-provided EAR/ITAR information is clearly labeled. Mark the cover page and page footers** containing export-controlled information **“ITAR/EAR-controlled: Do Not Distribute to Unauthorized Non-U.S. Persons.”**
* **Label** ITAR controlled items “ITAR.”
* **Label** devices containing data (e.g., flash drives, back-up hard drives) “ITAR” or “EAR” as appropriate.

## PRINTING

Retrieve documents immediately.

## DISPOSAL

Crosscut shred all controlled documents. When unavailable, use locked, university shred barrels.

Coordinate in advance with Export Control when disposing of export-controlled data on computers, portable digital media devices, or equipment.

TRAVEL

International travel for university business should always be registered in the [U of A International Travel Registry](https://ua-risk.terradotta.com/). Indicate you are on a TCP when completing the registration, even if traveling for an unrelated reason.

**If you plan to travel internationally with** export-controlled items/data, or to **access** export-controlled information electronically (email, cloud storage, etc.), it may require prior federal authorization and/or other paperwork and documentation. Notify Export Control prior to travel for potential license determination. Licenses take time to obtain, therefore notification should be made as soon as possible.

# INFORMATION SECURITY

University of Arizona policy requires all researchers to appropriately secure export-controlled digital data. Individuals who have signed this TCP are responsible for the secure maintenance and protection of all export-controlled data and information.

* **Lock and password protect devices** that contain export-controlled information.
* **REGULARLY UPDATE SOFTWARE** on computers accessing export-controlled data with manufacturer provided patches.

## ENCRYPTION

* Encrypt and password protect folders, files, and hard drives containing export-controlled data. Encrypt data while storing or transmitting.
* **Encrypt removable storage devices containing controlled data** at the file/folder level or at the device level with **FIPS 140-2 Level 2 or AES 256** standard encryption.
* **Encrypt emails and attachments** containing export-controlled data (distributed or received).
* Provide passwords separately via [Stache](https://stache.arizona.edu/) or similar secure method.
* **Indicate in the email subject** when the email or attachments contain export-controlled data.
* **Do not use student accounts to email controlled data**, unless using a “CatWorks” account. Regular student email accounts do not provide adequate encryption.
* Refer to [Encryption Guidance](mailto:https://research.arizona.edu/sites/default/files/2024-08/Encryption-Guidance-01.07.2021.pdf).

## REMOTE WORK AND OFF-CAMPUS DATA ACCESS

Accessing export-controlled data off-campus has increased risks, which include:

* Unknown levels of physical and cyber security.
* Limited University oversight of security levels.
* Reduced awareness of a possible breach.
* Greater potential for access by unauthorized individuals.

Personnel working from any off-campus location must consider these risks and assume responsibility for mitigation. Individuals who have signed this TCP agree to apply security measures such as:

* Do not work with controlled data in public spaces.
* Do not use public wi-fi hotspots to access export-controlled technical data.
* Establish a UA VPN connection to access data. Only use **vpn.arizona.edu/full** unless otherwise detailed in the TCP.
* Screen lock devices with a strong password.
* Do not permit other people in the room while reviewing data.
* Report any suspicious activity/theft to Export Control ([export@arizona.edu](mailto:export@arizona.edu)) as soon as possible.
* Report any circumstances that increase the chance of unauthorized access to protected information, including non-U.S. Persons residing in or frequenting the location, to Export Control ([export@arizona.edu](mailto:export@arizona.edu)).

## VIDEO CONFERENCES

**Always enable security features** (e.g., passwords, do not record, etc.) when using video platforms to discuss controlled data. Do not enable AI or recording features. Refer to [CISA Guidance for Securing Video Conferencing](https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf).

# PUBLICATIONS AND PRESENTATIONS

Check the Project details for any Sponsor related publication restrictions or procedures.

Regardless of Sponsor requirements, technical data (ITAR) and technology (EAR) for controlled items must be published in accordance with the regulations. Export Control will review and provide guidance. All ITAR technical data will go through an external government approval process prior to publication/dissemination.

# PROCUREMENT

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 compliance with U.S. export control laws and regulations.

* Refer to [Purchasing and Shipping](https://research.arizona.edu/compliance/export-control-program/purchasing-shipping) for specific guidance on processing University purchases.
* Obtain signed *Vendor Certification* forms. Keep the original documentation on file and available for review by Export Control. See Export Control’s [Liaison Toolbox](https://research.arizona.edu/compliance/export-control-program/liaison-toolbox-forms) for *Vendor Certification* forms.
* Run [Restricted Party Screening](https://research.arizona.edu/compliance/export-control-program/procedures-for-restricted-party-screenings) (RPS) on all vendors, including transactions paid by PCard. The University of Arizona will not do business with a vendor on a restricted parties list.
* Identify ITAR equipment on the Control Plan and label it “ITAR.” Only individuals who have signed this TCP are allowed access to ITAR-controlled equipment or items.

**NOTE: If a vendor is a non-U.S. entity, the Vendor Certification form mentioned above is not applicable; however, an export license could be required prior to providing technical specifications to the vendor.**

# SHIPPING/TRANSPORTING

When transporting documents, notes, materials, or encrypted export-controlled data, keep items secured and avoid stops at locations that are not included in the TCP.

* **Track** shipments of ITAR/EAR-documents or items. Confirm documents and items are labeled. Place items in an inner envelope/box/crate, etc. marked **“ITAR/EAR-CONTROLLED: NO NON-US PERSON ACCESS.”** Place inside an envelope, box, crate, or container for shipping or transporting with **no export-controlled markings**.
* Obtain documentation from the receiver on protocols confirming receipt of item by a U.S. Person or authorized non-U.S. Person.
* **Coordinate with Export Control before shipping export-controlled items/data internationally or transferring to non-U.S. Persons.**
* ITAR items ***will*** require a license. Do not ship until the license is approved and received by Export Control.
* EAR-controlled items ***may*** require a license. Coordinate with Export Control in advance for next steps.
* **Export Control will apply for all export licenses.** Regulations require copies of licenses and shipping paperwork and other documentation to be retained for five years after the expiration of the license. Provide copies of all shipping paperwork to Export Control. Consult a U of A approved customs broker prior to shipping equipment/items internationally.

# PERSONNEL SCREENING

Notify Export Control of changes in personnel. All personnel and all visitors with access to potentially export-controlled data, including visual access, are screened against U.S. Government restricted parties lists prior to receiving access. Refer to the University’s procedures for [Restricted Party Screenings](https://research.arizona.edu/compliance/export-control-program/procedures-for-restricted-party-screenings).

# TRAINING AND AWARENESS

All TCP personnel must complete Export Control training, participate in an Export Control briefing, and certify their understanding of this TCP ***before*** working on the project. Export Control will confirm when mandatory training requirements are met.

To remain on the TCP, biennial refresher training is required. Refer to [Training and Guidance](https://research.arizona.edu/compliance/export-control-program/export-control-training) on the Export Control website.

# REPORTING

Report any concerns and known or potential violations (giving a non-U.S. Person access to certain export-controlled data without the proper government authorization, if required) as soon as possible.

* **Potential Break In or other Crime on Campus:**
* Immediately call 911 to file a police report.
* Report to Export Control.
* **Potential Export Violation:**
* Remove unauthorized non-U.S. Person’s access.
* Report to Export Control.
* **Targeted Suspicious Contacts:** Report to Export Control and the [Facility Security Officer](https://research.arizona.edu/compliance-public/research-security/facility-security-officer-fso) any unusual communications from unknown individuals requesting:
* To work with you.
* Your assistance.
* Potentially sensitive information.

# COMPLIANCE ASSESSMENT

Complete regular self-evaluation and internal audits to review procedures and identify gaps and vulnerabilities.

Export Control conducts formal audits annually but may request more frequent check-ins to maintain compliance with the procedures.

Contact Export Control ([export@arizona.edu](mailto:export@arizona.edu)) with any questions or concerns related to this TCP.

# TERMINATION

This TCP remains in effect to protect the export-controlled items or information as long as they are retained or stored in any University location or system. Coordinate with Export Control on proper transfer or destruction of export-controlled equipment, software, and technical data.

Export Control retains all records of export-controlled items and documents related to export licenses/authorizations in accordance with U of A policy and applicable federal regulations.

# CERTIFICATION

I accept responsibility for the oversight of this Control Plan, participated in a briefing, and received a copy of this document. I had an opportunity to ask questions and agree to follow the procedures outlined in the Control Plan. I will coordinate all changes in locations, scope of work, and personnel with Export Control. I will share any concerns with Export Control. I understand that I could be held personally liable if I unlawfully disclose export-controlled information or items to unauthorized non-U.S. Persons.

|  |  |
| --- | --- |
|  |  |
| **Responsible Party Name** | **Date** |
|  | |
| **Responsible Party Signature**  **Date** | |

# APPROVALS

**University of Arizona Export Control approves this Control Plan.**

|  |  |
| --- | --- |
|  |  |
| **Export Control Name** | **Date** |
|  | |
| **Export Control Signature**  **Date** | |

# INDIVIDUAL SIGNATORY PAGE

I hereby certify that I participated in a briefing and received a copy of the Control Plan. I had an opportunity to ask questions and agree to follow the procedures outlined in this document. I will share any concerns with Export Control. I understand that I could be held personally liable if I unlawfully disclose export-controlled information or items to unauthorized non-U.S. Persons.

|  |  |
| --- | --- |
|  |  |
| **Signer** | **Date** |
|  |  |
| **Department** | **Status** |
|  | |
| **Signature** | |

# INTERNAL SELF AUDIT CHECKLIST

|  |  |  |  |
| --- | --- | --- | --- |
| Auditor: |  | Date: |  |
| 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/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