**OVERVIEW**

Your project has been identified as involving export controlled information, technology, or materials covered under either the [International Traffic in Arms Regulations (ITAR)](https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987) under the jurisdiction of the Department of State, or the [Export Administration Regulations (EAR)](https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear) under the jurisdiction of the Department of Commerce.

It is unlawful to send or take export controlled technology or materials out of the U.S., or to disclose it (orally or visually) or transfer it to a non-U.S. person *inside or outside the U.S.*, without proper authorization. Additionally, under the ITAR or the EAR a license may be required for foreign nationals to access or use it. A foreign person is a person who is not a U.S. citizen *or* permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

Technical information, data, materials, software, or hardware, i.e.; technology generated from this project/activity, must be secured from release/disclosure to unauthorized persons. Security measures will be appropriate to the classification involved and the format of the export controlled items. This Technology Control Plan (TCP) is intended to provide the necessary guidance and safeguards you are responsible for to prevent its unlawful disclosure or release.

The Office of Regulatory Services will facilitate development of a TCP and acquisition of an export license, if necessary. The Office of Information Technology will also provide input when a TCP involves export controlled data in an electronic format.

After a TCP is approved, the Office of Regulatory Services will perform an annual check-in to ensure that procedures are up to date and carried out according to the TCP. Additional monitoring may occur such as laboratory visits, inventory reviews, and evaluations of information security.

**For guidance on appropriate security precautions and completing the TCP document, see:** [**https://resources.uta.edu/research/regulatory-services/export-control/TCP%20Guidance.php**](https://resources.uta.edu/research/regulatory-services/export-control/TCP%20Guidance.php)**.**

This TCP contains CONFIDENTIAL information classified as [Category I (Confidential) Data](https://www.uta.edu/security/data_classification/).  The TCP must be maintained in a secure manner with access restricted to only University Administration and authorized personnel listed in this TCP.

1. **Principal Investigator** (name and contact information of the responsible individual for this project):

|  |
| --- |
|  |

1. **Background and Usage** (provide a technical description of the controlled item/material/technology/
equipment/software, and its planned use. Include USML # or ECCN # if available):

|  |
| --- |
|  |

1. **Support / Sponsorship** (reference appropriate Agreement(s) related to the controlled technology if applicable, such as a sponsored Project, NDA, MTA, etc.):

|  |
| --- |
|  |

1. **Receipt of Controlled Materials or Data** (describe how the controlled materials or data will be transmitted or transferred to you/UTA campus):

|  |
| --- |
|  |

1. **Physical Security Plan:** (project data and/or materials must be physically shielded from observation or use by unauthorized individuals by operating in secured laboratory/workspaces, or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of “work-in-progress”):
	1. **Location** (describe the physical location of each controlled technology / item including building and room numbers):

|  |
| --- |
|  |

* 1. **Physical Security** (provide a detailed description of your physical security plan designed to protect your item/technology/materials from unauthorized access, i.e., secure doors, locked cabinets, limited access, security badges, use of secure time blocks, etc.):

|  |
| --- |
|  |

* 1. **Conversation Security** (describe your plan for protecting export controlled information in conversations):

|  |
| --- |
|  |

1. **Describe Item Marking** (export controlled information must be clearly identified and marked as such. See [TCP Guidance](https://resources.uta.edu/research/regulatory-services/export-control/TCP%20Guidance.php) for sample language):

|  |
| --- |
|  |

1. **Information Security Plan:** Will your project involve controlled data, information, or materials in an electronic format (includes receipt, transfer, or storage)? [ ]  Yes [ ]  No

**If yes, complete this section. If no, skip to the next section.**

**Note:** Electronic data/information that is controlled is considered Category I of the Data Classification Guidelines. **The following standards must be implemented for Category I data, at a minimum:** [**https://www.uta.edu/security/policies/minimum.php**](https://www.uta.edu/security/policies/minimum.php)**.** In the prompts below, describe how you will comply with these requirements.

1. Describe the procedures that will be used for system hardening (e.g., firewall rules, turning on automatic updates, disabling unused applications/services, password restrictions, encryption, etc.).

|  |
| --- |
|  |

1. Describe the procedures that will be used to discard controlled data. See: <https://www.uta.edu/security/policies/secure_destruction.php>.

|  |
| --- |
|  |

1. Describe the process for system backup (e.g., crashplan, external drive, multiple hard drives) and who will have access.

|  |
| --- |
|  |

1. ***If applicable***, describe how controlled information will be securely accessed in a shared environment (e.g., database, cloud storage) and transmitted to/from collaborators, sponsors, and project personnel. See [TCP Guidance website](https://resources.uta.edu/research/regulatory-services/export-control/TCP%20Guidance.php) for information on cloud computing and encryption standards for legal transmission of EAR-controlled information and ITAR-controlled information.

|  |
| --- |
|  |

1. Explain how computers will be sanitized upon completion of the project.

|  |
| --- |
|  |

1. Describe the process for change management: (e.g., change control document, test environment).

|  |
| --- |
|  |

1. Will controlled information be stored on laptops, flash drives, or other portable devices? If yes, describe the devices, what information will be stored on them, and how the devices will be secured within the [effective control](https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=939a4fe6f48197894ec0ba7cc40885f9&term_occur=1&term_src=Title:15:Subtitle:B:Chapter:VII:Subchapter:C:Part:772:772.1) of an authorized individual.

|  |
| --- |
|  |

1. Please describe the logging capability of the systems or applications utilized (documentation, recording, or tracking of a user’s activity).

|  |
| --- |
|  |

1. Describe the computer virus protection (e.g., TrendMicro, Windows Defender) and any anti-spyware software that will be utilized.

|  |
| --- |
|  |

1. Who is your primary IT contact in the event of a problem? Please provide the name and contact information.

|  |
| --- |
|  |

1. Describe the IT Structure in the table below (the setup / system at each location that will have/store controlled information).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type ofInformationSystem (e.g., desktop, laptop, database) | Location | Asset Tag  | Managed By? (OIT, Locally Managed) | Encryption?(e.g., 128-bit orhigher) | Connectedto the UTA network? |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Travel:** Will there be any travel (**international or domestic**) that will require taking an export controlled item, material, or electronic data in any form? If yes, please list the destination(s), the purpose of taking controlled material, and how the controlled item(s) will be secured within your [effective control](https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=939a4fe6f48197894ec0ba7cc40885f9&term_occur=1&term_src=Title:15:Subtitle:B:Chapter:VII:Subchapter:C:Part:772:772.1) during the trip. Persons not authorized by this TCP are not permitted to access or use the controlled items. A license or license exception may be necessary to take the controlled items outside of the U.S., or to collaborate/share/allow access to a non-U.S. Person (Office of Regulatory Services will facilitate this). For international travel, please see the following guidance: <https://resources.uta.edu/research/regulatory-services/export-control/International%20Travel.php>.

|  |
| --- |
|  |

1. **Training:**
2. **Site Specific Training:** It is the PI’s responsibility to discuss the procedures of this TCP with all Project Personnel to ensure they understand their responsibilities. The PI must also create and maintain **documentation** of the site specific training for each individual having access to or working with controlled items/materials, including new personnel that are added to the project at a later time. Training documentation may be requested for compliance monitoring or university internal audit purposes.
3. **Other Training:** In addition to receiving site-specific training from the PI, each person listed as authorized personnel on this TCP will be familiar with the federal export control regulations <https://resources.uta.edu/research/regulatory-services/export-control/regulations.php>, UT Arlington’s Policy for Export Controls <https://resources.uta.edu/research/regulatory-services/export-control/index.php> and will complete the online training module “Export Control” <https://www.uta.edu/ra/real/researchspace.php?view=7>.
4. **Certification:** Each Authorized Individual will be required to read and understand the procedures of this TCP, and provide signature certification.  No additional personnel will have access to controlled material, information, or technology without approval by UT Arlington’s Responsible Official for Export Control (through amendment of this TCP).
5. Describe how you will fulfill the training requirements above:

	1. List who will be responsible for conducting site specific training:

|  |
| --- |
|  |

* 1. Describe the schedule and method for training, including for new personnel added in the future:

|  |
| --- |
|  |

* 1. Describe how site specific training will be documented (this documentation will be requested during annual follow ups or during audits, routine inspections, etc.):

|  |
| --- |
|  |

1. **Self-Evaluation Program:** It is the PI’s responsibility to continuously monitor the project for adherence to, and effectiveness of, the TCP. Any violations or deficiencies must be reported to the Office of Regulatory Services. The TCP may be modified (via a TCP Amendment) to provide appropriate protection.  Modifications will be coordinated and approved by the Responsible Official for Export Control prior to implementation.
2. **Self-Evaluation Schedule** (describe how often you plan to review / evaluate your TCP):

|  |
| --- |
|  |

1. **Audit Checklist** (provide a checklist for items to be reviewed during self-evaluation audits):

|  |
| --- |
|  |

1. **Documentation** (describe how self-evaluations will be documented, to include at minimum the date of the evaluation and the items evaluated. This documentation will be requested during annual follow ups or during audits, routine inspections, etc.):

|  |
| --- |
|  |

1. **Completion of Project and Disposition of Controlled Items:** Describe the anticipated or estimated length of this project and explain the disposition of the controlled information/materials/technology at the conclusion of the project (e.g., materials will be returned or transmitted back to the sponsor; hard copies will be shredded; electronic data will be destroyed, etc.). See UTA guidance for secure media destruction and erasure: <https://www.uta.edu/security/policies/secure_destruction.php>.

|  |
| --- |
|   |

1. **Project Personnel & Certifications** (In the table below, list every person who will be authorized to access the controlled information / materials / technology).

**\*Each person signing below certifies that their citizenship status provided in this document is correct and that they have read, understand, and will adhere to the terms of this Technology Control Plan. If citizenship or employment status changes after approval of this TCP, Regulatory Services must be** [**contacted**](https://resources.uta.edu/research/regulatory-services/index.php)**.**

**Principal Investigator:** Through signature below, the PI certifies responsibility for: oversight of the project and its personnel, monitoring compliance with the procedures of this TCP and applicable export control regulations, ensuring personnel are properly trained, promptly reporting any violations or deviations from the TCP, and fulfilling and maintaining all recordkeeping requirements of the TCP.

**Training & Awareness**: You must (1) read and adhere to the procedures of this TCP & subsequent Amendments, (2) complete site-specific training prior to your access or work with controlled items/materials, (3) complete the [online Export Control training](https://research.uta.edu/ra/real/loginscreen.php?page=%2Fra%2Freal%2Fresearchspace.php%3Fview%3D7) module, and (4) be familiar with and adhere to any applicable EAR and/or ITAR [regulations](https://resources.uta.edu/research/regulatory-services/export-control/regulations.php).
**Reasonable Care**: You may be held personally liable for violations of the ITAR or EAR. As a result, you must exercise care in using Export-Controlled Information, Technology, or Materials. Controlled Items must be handled in accordance to the security plans and/or controls specified in this TCP and only be shared with authorized Project Personnel. Unsecured Export-Controlled Information or Materials should not be left unattended. You must not travel internationally with any controlled information, technology, or materials without first consulting the Export Control Officer. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled Information up to and including incarceration. If you have any questions or concerns, contact regulatoryservices@uta.edu or 817-272-3723.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Email** | **UTA ID number** | **Completion Date of Online Training**  | **Citizenship Status (U.S., non-U.S., Permanent Resident)** | **Role/Status (faculty, staff, student, non-UTA collaborator)** | **UTA Employee?****(Yes/No)** | **Signature & Date** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\*\*OFFICE USE\*\*
Approval of TCP:**

**OIT Approval Date, if applicable:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
**Jeremy Forsberg, Assistant Vice President for Research Date
UTA Responsible Official for Export Control**