UNIVERSITY OF Cincinnati

TECHNOLOGY CONTROL PLAN

The Technology Control Plan ("TCP") details the established measures to ensure compliance with restrictions imposed by U.S. laws and regulations. These restrictions may pertain to a university, company, and or government sponsor's' proprietary and or export controlled information or "commodities". The TCP outlines the security procedures required for the performance of restricted work that safeguard and control access to information and or "commodities" that are export controlled pursuant to the International Traffic in Arms Regulations ("ITAR") 22 CFR § 120-130, and the Export Administration Regulations ("EAR") 15 CFR § 300 – 799. The controls will cover the physical and electronic procedures for access, use, storage, transfer (deliverables) and destruction. The principal investigator/responsible individual will provide the information for each section and certify to acceptance.

UC is fully committed to compliance with all applicable export control laws, regulations and sanctions. Violation of export control laws may be punishable by severe fines and penalties including imprisonment and debarment from federal contracting.

Department to retain documentation for 5-years from project completion, or from expiration of the license (as applicable)[1]

Principal Investigator / Responsible Individual:	**Contact Information:**
Sponsored Program / Project Title:	**UC Proposal / Award / Contract Number:**
Prime Sponsor:	**Military/Government Agency Sponsor:**
USML Cat. / ECCN:	**Department Head:**

If restrictions are listed on foreign person/nationals participation, identify where: Page(s)_____and Section(s) _____
If restrictions or clauses are listed (e.g. proprietary, export controlled, confidential, etc.), identify where: Page(s)_____and Section(s) _____

Revision #	Revision Date	Modifications	Signature of ECO Approval
Original		TCP developed and implemented	

[1] Retention requirement: EAR 15 CFR Ch. VII, §762.2 - 762.7; ITAR 22 CFR §122.5 and §123.26. See also 15 CFR § 30.10

Research Participants

List all personnel[2] (staff, faculty, students, contractors, including visiting persons) includes paid & unpaid persons.

Name	Title	Home Institution/Employer	Citizenship	RPS Conducted*

*Restricted Party Screening conducted in Visual Compliance by authorized UC staff.

Project Description

Clearly define the activities, technical data, hardware, and or defense services. Include background information on the full scope of the program and summary of the statement/scope of work.

[2] All participants must complete online training and Appendix A

Commodities and Technical Data

List all items that will be used in the project (e.g. equipment, software, source code, algorithms, drawings, etc.) with their restriction level if known (confidential, proprietary, sensitive but unclassified, classified, export controlled). Include items on-loan or temporarily on campus (e.g. for testing, review, etc.) as well as permanent.

Item (Make/Model #)	Description	Restriction Level	Manufacturer /Owner	ECCN / USML Category[3]	Purchased for this project (Y/N)[4]	Do you plan to export it from the U.S.? (Y/N)

If controlled select agents and/or toxins will be used, please provide below:

Name of Select Agent / Toxin	Quantity (mg)	ECCN/USML

Security Controls

Identify the location of all items listed above and storage details. If all items will be in same location, only list it once with "all" in the item column.

Item	Building Name	Lab/Room/Office	Building Address	Access Control Type	Established with Campus Security?

[3] Obtain the export classification from the sponsor/supplier/manufacturer or work with the Export Office to classify UC developed items

[4] If any items will be purchased, ensure you obtain the export classification from the supplier/manufacturer and attach supporting documents to TCP submission.

How is room access controlled and monitored:

If you are controlling access with keys, list who has copies, key number:

Is the area shared with other faculty, staff, students, groups? If yes, please list who and their project/activity if known:

In regards to technical data, what is the marking or identification of the documents?

Identify all electronic devices where technical data will be used/ stored (e.g. computers, laptops, USB drives, tablets, external hard drives, CDs, etc.)

Make / Model	Serial #	User	Owner	Storage location when not in use (locked cabinet)

How will the information be removed from the device(s)? Are you working with UC Information Security for removal?

International Travel

If there is any projected international travel for this project, please list details below:

Name	Dates	Country(ies)	Reason for trip	Taking UC equipment (e.g. laptop, samples, prototypes, etc.)

Reporting

Any request for information pertaining to this project must be immediately reported to the Export Control Office, including visits by law enforcement (FBI, DHS, DOS, DOC, etc.). The project data is protected under US laws and any disclosure must be reviewed and approved prior to release.

Immediate reporting of possible incidents is required. The following are examples of possible incidents that should be reported immediately and steps must be taken to ensure compliance:

Inadvertent or deliberate:

- Access by unauthorized persons
- Disclosure of data or hardware by any means: e.g. email, uploading to website, tour of controlled area, conversation, observation of ITAR controlled items/process, etc.
- Access to project data on an unsecure device or at an offsite location not previously approved
- IT system(s) breached or Hacking attempts
- Shipment of export controlled item(s)
- Any other suspicious activities

You may directly report the possible incident to the Export Controls Office, Office of General Counsel, or the Hotline at 1-800-889-1547.

Completion of the Project

All commodities (technical data, hardware, equipment, etc.) must be properly stored as stated in this plan until they are ready for disposal. Once the items are ready for disposal proper steps must be taken to ensure compliance. All technical data that is no longer needed on the electronic devices must be effectively wiped (contact your department Information Security administrator or UC Info Security for information/assistance) or paper must be shredded. All controlled equipment, hardware; items must be properly returned or disposed. The Export Controls Office is able to assist with the proper procedures to ensure appropriate disposal.

Project Personnel Certification

All personnel must certify that they have not disclosed any information, documents, or other items subject to this project to unauthorized persons. A certification must be submitted upon removal or departure from this project, UC, or the completion of the project.

Technology Control Plan Submission:

I certify that the information contained within the Technology Control Plan is accurate and truthful to the best of my knowledge. I am fully committed to following this plan to the best of my ability as I am committed to adhering to U.S. laws and regulations and the protection of controlled commodities. I understand the procedures outlined in this TCP and will notify the export control office immediately if further clarification is required. I will protect all items that are considered restricted (e.g. proprietary, confidential, sensitive, export controlled, etc.). I further certify that all participants will:

Complete online export control training and the certificate of completion will be submitted.
Receive notification of controlled items prior to access (proper labels/identification).
Certify that they understand the TCP and will be supervised by me or a designated person (identified below).

The TCP will be monitored and reviewed periodically to ensure accuracy. When there are changes, items or personnel, an amended TCP will be submitted for review and approval.

Signature **Date**

Name, Title _____

Department and College _____

University of Cincinnati

APPENDIX A

Non-Disclosure Statement and Confirmation of Understanding TCP

To be completed after online training, please submit the certificate of completion with this document.

Approved Personnel

I certify that I have completed export control training and understand the requirements of the U.S. Export Control Regulations. I understand that any technical data, commodities (e.g. equipment, prototypes, etc.) and defense services that are subject to the United States Munitions List (USML) and or the Commerce Control List (CCL), that I may have access to or may be disclosed during my participation on this project, are subject to export control under the International Traffic in Arms Regulations (ITAR) and or Export Administration Regulations (EAR).

I understand that I may be held personally liable for any unlawful disclosure to unauthorized persons. I certify that I will not disclose or export in any form the controlled information or commodities (e.g. materials, software, source code, equipment, etc.) to any person. If I inadvertently disclose or export any controlled technical data or commodities, I will immediately report the incident to my supervisor or Principal Investigator and the UC Export Control Office.

I further certify that I understand the requirements of this Technology Control Plan for the project and I agree to the provisions provided therein. My supervisor or Principal Investigator has clarified any questions or concerns. I understand that I will have to attend export control training annually for the duration of my employment[5] (paid or unpaid) on this project.

Participant Signature:_____ **Date:**_____
Name and Title
University Name

Supervisor/Principal Investigator Signature:_____**Date:**_____
Name and Title
University of Cincinnati

[5] Employment encompasses any of the following: assignment, visit, researcher, enrollment, employee, etc.