UNIVERSITY of WISCONSIN
UWMILWAUKEE
Office of
Sponsored Programs

EXPORT CONTROLS PROGRAM

AUGUST 2022

Technology Control Plan

1. Institutional Commitment

The University of Wisconsin-Milwaukee is committed to complying with export control laws, which are federal regulations that control the conditions under which certain information, technologies, and commodities can be transmitted overseas to anyone, including US citizens, or to a foreign national on U.S. soil. The university is also committed to complying with access and distribution restrictions imposed by federal committed to complying with access and distribution restrictions imposed by federal sponsors to facilitate control, distribution, and release of certain information for reasons of national security. This Technology Control Plan (TCP) is written explicitly for all export controlled items or information received or generated by UWM faculty, staff, students (UWM Personnel), and describes the specific measures that will be taken by the Responsible Person.

Questions related to the implementation of this TCP or the obligations of project personnel with respect to this TCP should be directed to the Responsible Person listed below. The Responsible Person and project personnel may also seek guidance from the Office of Sponsored Programs.

Responsible Person: _____________

Department: ___________________

Project Personnel: _______________________________

2. Project Information

This TCP applies to the following project:

Project Title/Project #: ___________________________________

Sponsor: ____

Responsible Person Contact Information:
Telephone Number: _____________________________
Email address: _________________________________
Building/room location(s) where project will be performed:_____________________

Please provide a brief overview of the project. Describe what sensitive data and materials will be provide and how they will be delivered:

Applicable EAR/ITAR Classification(s), if known: ____________________________

3. Security

Appropriate security of security sensitive and/or export-controlled items and/or information requires that, at minimum, project personnel adhere to the “one lock” principle. This principle requires that all security sensitive and/or export-controlled items or information be secured by using at least one mechanism to prevent access by unauthorized persons. This section outlines the methods required to achieve "one lock" security with respect to both physical and information security.

Physical Security

Physical security requires:

- Protecting materials (physical or digital) in order to ensure that project materials stay within secured areas (including via any network).
- Securing all export-controlled data in a locked room, storage device, or container when not in the personal possession of project personnel.
- Export-controlled items, if they are hardware assemblies or their equivalent, must be protected with seals to easily identify any evidence or physical tampering.
- Ensuring that all work is performed within secured areas.
- Marking all physical materials (i.e., hardcopy, removeable media, etc.) as export-controlled, proprietary, and/or subject to an NDA, as applicable.
- Ensuring that only project members are present in secured areas when work on this project is being performed.
- Preventing non-U.S. person from viewing or having access to any project data (physical or digital) or secured area (including for purposes of activities that are not project-related, such as maintenance or cleaning), unless such foreign national are: 1) project personnel and 2) have either obtained a license form the Department of Commerce and/or State, as applicable, or the university determines that there is a license exemption or exception under applicable regulations.
- Verifying that physical access for server operations, maintenance and repair will be restricted to individuals who have completed TCP Awareness Training, are authorized to receive all technical data stored on the server, and whose job responsibilities reasonable require such access.

[Description of physical security]

Information Security

Information security requires:

- Adherence to any requirements outlined in the relevant contract/NDA, such as technology controls, data classification, encryption, network access, non-disclosure, and secure destruction. If the relevant contract requires adherence to DFARS 252.204-7012, adherence requires completion of a cybersecurity standard assessment. Consult with your local IT administrator for assistance.
- Using encryption to send data over any networks. All data stored on computers and removable media must be encrypted at rest, utilizing a whole disk encryption product wherever feasible.
- Drives and devices used to store export controlled information must be password protected or encrypted. For data storage on drives with network access or back-up servers, export controlled information must be secured by both encryption and password protection.

- Project computers should be non-networked unless network connectivity I required for project work. If network connectivity is required, project computers should be configured to deny all non-essential inbound and outbound traffic.
- Limiting use of computers and servers containing export-controlled information to approved project personnel who have executed a certification that they have been made aware of the requirements of this TCP and agrees to comply with it as well as all applicable export control regulations.
- When project computers reach their useable life, physical media (i.e., Hard drives, USB drives, etc.) must be forensically erased or destroyed.
- Avoid usage of supercomputing or cloud computing facilities or services to store, process, or transfer export controlled information.

Please describe the information security controls that will be used to prevent unauthorized access to project-related information:

[Description of information security]

4. Personnel Screening

UWM employees will be screened against the Consolidated Screening List.

The personnel assigned to the project are:

[List full time personnel and U.S. Citizen or Visa status]

Part Time personnel who will participate in this research but are not funded by it are:

[List part time personnel and U.S. Citizen or Visa status]

Training and TCP Awareness

All personnel working on the project, funded, non-funded, full time or part time, are required to be notified of the export controlled information or materials. They should be provided the appropriately filled out letter in Appendix A and provide their signature. A refusal would result in the inability to work on the project in any capacity.

[List training on controlled materials and information required for all personnel.]

5. Publication/Graduate Theses

The Responsible Person and all project personnel must ensure that no Export Controlled items or information are included in a thesis or other publication. The Responsible Person also must ensure that all project personnel adhere to sponsor review requirements associated with any project subject to this plan. While it is the university's intent to protect unfettered rights to publication, this may not be possible on projects subject to this TCP.

Student participation on projects that required the sponsor's permission to publish or where results are subject to US export controls must be limited to work which is not required for the completion of their degree or program. Students may have access to background proprietary information only to the extent permitted by the applicable export control regulations.

6. End of Project Security Measures

a. UWM generated Export Controlled items or information:
The Responsible Person must dispose of or appropriately secure all export-controlled items and information at the end of the project. Electronic files must be purged from the hosting device or appropriately secured using standard file management tools. Please contact your local IT administrator for guidance.

b. Third Party generated Export Controlled items or information:
The Responsible Person must return all Export Controlled item or information to the disclosing party, or parties, at the close of the contract under which such information or items were received, or to the parties that transmitted such information unless there is a legitimate business or research-related reason for retaining such items or information.

7. Reporting Violations

All instances of non-compliance with the requirements of this TCP must be reported immediately to the compliance manager. The incident report should identify all relevant information, including but not limited to the date and nature of any disclosure or export; the name(s) of the person(s) involved; and a description of the disclosed or exported items or information.

Responsible Person:

____
[Name and title] Date

Office of Research:

____
[Name and title] Date

ATTACHMENT A

Project Name:____

This is to acknowledge that I have been briefed that this TCP applies to the project listed above. I understand that my participation on this project may involve the receipt or use of export controlled technology, items, software hardware or technical data and that it is unlawful to transfer, send or take export controlled materials or technology out of the United State. Furthermore, I understand that I may not disclose, orally or visually or transfer by any means, export controlled technology or technical data to a non-US Person located inside or outside the US without a license or applicable exemption. I understand that all non-US students, visitors, staff, post-docs or any other person must receive preauthorization consistent with the requirements of this TCP before accessing export controlled materials or data. I have discussed this TCP and its requirements with the Responsible Person for this project and I agree to follow all of the procedures contained in the TCP. If I have any questions about the applicability of the TCP to this project I will contact the Responsible Person for guidance.

Signature: _______________

Printed Name: _____________________

Date: _______________________