Office of Export Controls

University of Missouri-Columbia

Standard Operating Procedure

Technology Control Plans

Technology Control Plans

Effective Date: August 8, 2017
Original Approval Date: August 8, 2017
Revised Date: N/A

Approved By: Michele Kennett
Associate Vice Chancellor for Research

Table of Contents

1.0 Purpose

To describe the role of a Technology Control Plan (TCP) in restricted research at MU and the circumstances and process involved when one must be implemented.

2.0 Scope

The SOP applies to all MU activities where laws, regulations, best practices, or University policy requires that export controlled (EC) information, technology, or equipment; Controlled Unclassified Information (CUI); or Controlled Technical Information (CTI) be protected from disclosure to unauthorized personnel. The activities controlled by a TCP may include specific research projects or the use of University space to safeguard (1) controlled information from various projects or (2) controlled materials and/or equipment. A TCP ensures all personnel involved understand their obligations under the export control laws and regulations.

A TCP supplements but does not supplant procedures to safeguard (1) classified information as proscribed in the National Industrial Security Program Operating Manual (NISPOM) or (2) critical program information as set forth in any applicable Operations Security (OPSEC) contractual requirements.

3.0 Policy/Procedure

Development

If the OEC determines a TCP is needed, the OEC will work with the PI to develop and implement a TCP to secure the controlled technology from access by unlicensed non-U.S. citizens. The TCP will include:

- a commitment to export controls compliance;
- identification of the relevant export control categories and controlled technologies;
- identification of the project's sponsors;

- identification and nationality of each individual participating in the project;
- appropriate physical and informational security measures;
- personnel screening measures; and
- appropriate security measures for and following project termination.

Appropriate Security Measures

The TCP will include physical and informational security measures appropriate to the export control categories involved in the project. Examples of security measures include, but are not limited to:

- Laboratory Compartmentalization. Project operation may be limited to secured laboratory areas physically shielded from access or observation by unauthorized individuals. These areas must remain locked at all times.
- Time Blocking. Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access.
- Marking. Export controlled information must be clearly identified and marked as export-controlled.
- Personnel Identification. Individuals participating in the project may be required to wear a badge, special card, or other similar device indicating their access to designated project areas. Physical movement into and out of a designated project area may be logged.
- Locked Storage. Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key-controlled access. Soft and hardcopy data, lab notebooks, reports, and other research materials should be stored in locked cabinets.
- Electronic Security. Project computers, networks, and electronic transmissions should be secured and monitored through User Ids, password controls, 128-bit Secure Sockets Layer encryption or other federally approved encryption technology. Database access should be managed via a Virtual Private Network.
- Confidential Communications. Discussions about the project must be limited to the identified and authorized project participants, and only in areas where unauthorized individuals are not present. Discussions with third party sub-contractors must occur only under signed agreements which fully respect the non-U.S. citizen limitations for such disclosures.

Execution & Certification

For projects requiring a TCP, OSPA cannot set up an account and no funds can be expended prior to OEC approval. Such approval will take the form of a final TCP that has been signed by both the PI and the OEC, a copy of which will be provided to OSPA by the OEC. All persons working on a TCP-controlled project, and any other individual requesting access to controlled space, equipment, or materials protected by a TCP, must read—or be otherwise briefed on the procedures outlined in—the TCP and certify his or her agreement to comply with all security measures outlined in the TCP. At such time as any person working on a project subject to a TCP no longer requires access to controlled information, equipment, or technology, s/he will certify (1) that no unauthorized disclosures were made and (2) a commitment to ongoing compliance subsequent to work on the project.

Training

Project personnel will be provided export compliance training by the OEC as outlined in the TCP. Additional training is available upon request.

Closeout

Upon termination of a project under a TCP, the OEC and the PI will work together to determine the status of any controlled information, equipment, or technology that was received in order to perform work, or generated under the project. Any such controlled materials must be returned to the sponsor, destroyed, or—if the PI wishes to retain those materials—the TCP will be modified as appropriate to ensure that adequate security measures are maintained to restrict access and prevent unauthorized disclosure.