

Export Controls and Sanctions – Standard Operating Procedures

Export Controls and Sanctions SOP #003: Technology Control Plans Version 1.0 – December 17, 2023



INTRODUCTION

This Standard Operating Procedure (“SOP”) outlines the processes and procedures used by the Export Control Officer (ECO) for implementing, maintaining, auditing, and closing Technology Control Plans (TCPs).

PURPOSE

The University of Missouri-Kansas City (UMKC) may come into possession of or generate export controlled technical data, technology, software or highly controlled items which need to be protected from visual inspection. With the volume of foreign persons on campus and the openness of an academic environment, the risk of a deemed export occurring is high. A deemed export occurs when export controlled technical data or technology is transferred to a foreign person while inside the U.S. In certain circumstances, the University may need to obtain an export license or utilize an export license exemption, if eligible, to perform certain deemed exports. TCPs are implemented to mitigate this risk by outlining safeguarding procedures for researchers to ensure that access is restricted to only personnel who have been approved by the ECO so that the ECO can verify their eligibility to access export controlled technical data, technology, or software and to ensure the appropriate governmental approvals are in place.

SCOPE

To facilitate compliance with applicable U.S. Export Controls and Sanctions regulations, TCPs will be implemented in accordance with the [UM System Export Compliance Management Program](#).

PROCEDURE

When a TCP is necessary to safeguard export controlled items or information, the ECO works with the Principal Investigator (PI) and Information Services (IS) to develop the TCP, ensures that the terms of the TCP adequately protect export controlled items or information, and saves records in accordance with UMKC Export Controls and Sanctions SOP# 001 Recordkeeping. The ECO follows the TCP throughout its lifecycle, ensuring compliance with the TCP, export control regulations, and relevant security-related contractual requirements.

RESPONSIBILITIES

The ECO is responsible for:

- Working with the PI, or other researchers, as appropriate, to accurately determine the export classification of export controlled items or information.
- Collaborating with the PI and IS to design a TCP that meets the needs of the researchers while also ensuring compliance with export control regulations and other relevant security-related contractual requirements.
- Validating citizenship for all persons accessing export controlled information.
- Performing a restricted party screening using the UMKC restricted party screening tool.

- Ensuring that a license determination is performed for all exports facilitated by UMKC.
- Ensuring that export license exemptions/exceptions are utilized correctly and that appropriate records of these are maintained.
- Partnering with the Director of Research Security and Compliance in the event that a license application needs to be submitted.
- Ensuring that TCPs are signed by the PI and their supervisor.
- Ensuring that all persons accessing export controlled information have: 1) received a TCP briefing; 2) completed CUI training prior to access and annually thereafter, as required; and 3) signed an **Acknowledgement of TCP** form.
- Maintaining records of briefings and CUI training.
- Updating TCPs as needed.
- Auditing and monitoring TCPs on a regular basis.
- Closing out TCPs once export controlled information is no longer at UMKC.

The PI listed on a TCP is responsible for:

- Providing technical expertise to the ECO to facilitate the accurate determination of export classifications.
- Sharing workflows and IT resource needs with the ECO and IS.
- Providing a list of all persons intended to work with export controlled items/information at the time the TCP is established and maintaining that list throughout the lifecycle of the award by communicating changes to the ECO.
- Attending TCP briefings and completing CUI training, as required.
- Otherwise following all terms of the TCP.

IS is responsible for:

- Working with the ECO and the PI to identify the best way to secure electronic format export controlled information that meets the needs of the researchers while also ensuring compliance with export control regulations and other relevant security-related contractual requirements.
- Provisioning access to electronic format export controlled information only when it has been approved by the ECO.
- If electronic format export controlled information needs to be deleted from any information system, ensuring that the data is adequately deleted in accordance with export control regulations and other relevant security-related contractual requirements.

Personnel authorized to access export controlled items and information on a TCP are responsible for:

- Attending TCP briefings and completing CUI training, as required.
- Otherwise following all terms of the TCP.

TCP IMPLEMENTATION

The following steps are provided as a general guide to assist the ECO to implement a TCP:

S1. When creating a new TCP, gather data from the PI to assess their research needs. This may be accomplished through the use of the **TCP Prep Questionnaire** or may be gathered through a conversation with the PI. Ensure that IS is part of all emails and conversations during this timeframe since they have a role in ensuring that information systems are configured appropriately.

S2. Using the information gathered, create an initial draft TCP by editing the **TCP Template** and customizing it for the needs of the project while confirming it still ensures compliance with export control regulations and security-related contractual requirements. Using the proposed list of people who will access export controlled items, technical data, or technology, validate their eligibility to gain access.

1. Is anyone on a restricted party list that would prohibit their access to export controlled items, technical data, technology, or software covered by the TCP?
 - a. If yes, notify the PI that an export license will be required for the restricted party to access the export controlled item(s), technical data, technology, and/or software covered by the TCP. If the University would like to proceed with obtaining an export license, contact the UM System Director of Research Security and Compliance.
 - b. If no, proceed to S2.2.
2. Are they a Foreign Person?
 - a. If yes, proceed to S2.3.
 - b. If no, proceed to S2.5.
3. Is an export license required?
 - a. If yes, proceed to S2.4.
 - b. If no, proceed to S2.5.
4. Is an export license exemption/exception available?
 - a. If yes, proceed to S2.5.
 - b. If no, notify the PI that an export license will be required for the foreign person to access the export controlled item(s), technical data, technology, and/or software covered by the TCP. If the University would like to proceed with obtaining an export license, contact the UM System Director of Research Security and Compliance.
5. Add personnel names to the TCP.

S3. Send the TCP draft to the PI and IS for review to ensure that the TCP adequately reflects the agreed upon security measures.

S4. Edit the TCP draft in accordance with feedback from the PI and IS while also confirming that any updates also ensure compliance with export control regulations and security-related contractual requirements.

S5. After reaching a consensus with the PI and IS, send the TCP to the PI for signature and send the TCP to their next level supervisor for signature.

S6. Provide a copy of the TCP to all project personnel and ensure that all project personnel (including the PI) receive a TCP briefing and take any other relevant security training required by the contract, including but not limited to, CUI training. Obtain signed **Acknowledgement of TCP** forms from all personnel who are listed on the TCP, except for the PI who signs the TCP directly. If there are any foreign persons qualifying for an export license exemption/exception, ensure all paperwork required for the export license exemption/exception is completed.

S7. Save all records of the TCP, TCP briefing, relevant trainings, signed acknowledgement forms, and required export license exemption/exception paperwork in accordance with UMKC Export Controls and Sanctions SOP# 001 Recordkeeping.

TCP MAINTENANCE

TCPs are intended to be living documents. During the course of work with export controlled items, technical data, technology, and software the needs of the PI may change. As such, make updates to the TCP to support these research needs. Minor changes will not require the TCP to be re-signed; however, larger changes may require additional meetings with the PI and IS and may require the TCP to be redrafted and resigned.

S1. Is the change only adding a new project number onto an existing TCP or removing someone from the TCP?

1. If yes, update the TCP and ensure all people listed on the TCP receive a revised copy of the TCP. No further action is required.
1. If no, proceed to S2.

S2. Is the change adding someone new to the TCP?

1. If yes, proceed to S3.
2. If no, proceed to S6.

S3. Validate eligibility to gain access for all new personnel.

1. Is anyone on a restricted party list that would prohibit their access to export controlled items, technical data, technology, or software covered by the TCP?
 - a. If yes, notify the PI that an export license will be required for the restricted party to access the export controlled item(s), technical data, technology, and/or software covered by the TCP. If the University would like to proceed with obtaining an export license, contact the UM System Director of Research Security and Compliance.
 - b. If no, proceed to S2.2.
2. Are they a Foreign Person?
 - a. If yes, proceed to S3.3.
 - b. If no, proceed to S3.5.
3. Is an export license required?
 - a. If yes, proceed to S3.4.
 - b. If no, proceed to S3.5.
4. Is an export license exemption/exception available?
 - a. If yes, proceed to S2.5.
 - b. If no, notify the PI that an export license will be required for the foreign person to access the export controlled item(s), technical data, technology, and/or software covered by the TCP. If the University would like to proceed with obtaining an export license, contact the UM System Director of Research Security and Compliance.
5. Add personnel names to the TCP.

S4. Ensure new personnel receive a TCP briefing and take any other relevant security training required by the contract, including but not limited to, CUI training. Obtain signed **Acknowledgement of TCP** forms from all new personnel who will access export controlled items, technical data, technology, or software covered by the TCP. If there are any foreign persons qualifying for an export license exemption/exception, ensure all paperwork required for the export license exemption/exception is completed.

S5. Add the names of the new personnel to the TCP and ensure all people listed on the TCP receive a revised copy of the TCP. No further action is required.

S6. Using the most recent version of the TCP, edit the TCP in accordance with feedback from the PI and IS while also confirming that any updates also ensure compliance with export control regulations and security-related contractual requirements. Send the TCP draft to the PI and IS for review to ensure that the TCP adequately reflects the agreed upon security measures.

S7. After reaching a consensus with the PI and IS, send the revised TCP to the PI for signature and send the revised TCP to their next level supervisor for signature.

S8. If significant changes were made to the TCP, consider ensuring all personnel receive a new TCP Briefing. Ensure all personnel listed on the TCP receive the revised TCP.

Note: There may be other scenarios where a change is minor enough that the TCP does not need to be redrafted and re-signed. Use your best judgement when determining whether to update a TCP without signatures or whether to require signatures on an updated TCP.

TCP AUDITS

TCPs must be regularly audited/monitored to ensure compliance with export control regulations. During the course of the audit, the ECO may uncover deficiencies or instances of non-compliance with the TCP. These will be mitigated and addressed, as appropriate. If any instances of non-compliance rise to the level of a violation of export control regulations, contact the UM System Director of Research Security and Compliance immediately.

S1. Begin going through the **Annual Review Checklist** to identify whether there are any deficiencies that need to be addressed. Prepare the **Annual Review Template**.

S2. Partner with the PI to discuss the project. Highlight any deficiencies that have already been identified. Gather information about whether any of the terms of the TCP are difficult to comply with and need to be adjusted to meet the needs of the PI. Discuss any upcoming changes the PI thinks may be about to happen with the project. If the project has ended, discuss whether there is still data not yet approved for public release at UMKC. This may be best in the format of a meeting or in an email depending on the scenario and the PI. Use your best judgement.

S3. Make any necessary updates to the TCP in accordance with the TCP Maintenance procedures above.

S4. Complete the **Annual Review Checklist** and **Annual Review Template**. Provide the **Annual Review Template** to the PI in case they would like to maintain a record of it.

TCP CLOSURE

When all export controlled items, technical data, technology, and/or software being protected by a TCP are no longer export controlled and/or are no longer at the University, the TCP should be closed.

S1. After a project has ended, contact the PI to see if export controlled items under the protection of the TCP are still at the University. Clarify what happened to the items (i.e., they been approved for public release, the been returned to the project sponsor and are no longer at the university, they have been deleted or destroyed such that they cannot be reconstructed).

Depending on what the export controlled item, technical data, technology, or software was and its format, and depending on the contractual requirements, there may be different standards for ensuring destruction or deletion. Do any export controlled items, technical data, technology, or software protected by the TCP remain at the University?


1. If yes, the TCP remains open and continues to be monitored until there are no more export controlled items, technical data, technology, or software at the University.
2. If no, proceed to S2.

S2. Provide the PI with a copy of the **TCP Close Out Certificate** customized to describe the method by which all items, technical data, technology, or software under the protection of the TCP no longer require protection.

S3. After the PI signs the **TCP Close Out Certificate**, close the TCP.

RECORDKEEPING

All export control recordkeeping will be managed by the Export Control Officer in accordance with SOP #001: Recordkeeping.

Previous Version Dates:	N/A
Signed by:	 Anthony Caruso, Ph.D. 12/17/2023 Interim Vice Chancellor for Research