# Request for Export-Control Exception to Open Research Policy MIT Technology Control Plan (TCP)

## Part 1: Technology Control Plan Summary

|  |  |
| --- | --- |
| **Responsible Individual (RI):** |  |
| RI Title: |  |
| Department, Lab or Center: |  |
| Email Address: |  |
| Request Date: |  |
| **Project Title[[1]](#footnote-1):** |  |
| **Proposal #** |  |
| Expected Project Duration[[2]](#footnote-2) |  |
| **Description of Export-Controlled Item:** |  |
| Item Type | Technical data  Technology  Software  Tangible item |
| Controlling Agency | State  Commerce  Treasury  Energy  Nuclear Regulatory Committee (NRC)  Homeland Security |
| Item Classification  e.g. Export Control Classification Number (ECCN), USML (ITAR) category | ECCN:  USML Category: |
| **Location of export-controlled item:** | Building:  Room #: |
|  |

## Part 2: Technology Control Plan

## MIT Policy and U.S. Export Control Law

[MIT Policy 14.2](https://policies.mit.edu/policies-procedures/140-research-policies-and-public-and-private-support/142-open-research-and-free) supports the free and open interchange of information among scholars and minimizes limitations on the participation of international faculty, students, and scholars. Limited exceptions requiring review and approval by the Vice President for Research are made when the research is crucially important to MIT's educational mission. MIT prohibits highly restricted export-controlled items (e.g., technology, software and tangible items) on campus unless a Technology Control Plan (TCP) has been approved. The Responsible Individual (RI) identified in the TCP is a MIT faculty or staff member. That RI is legally responsible for complying with U.S. export control laws while the export-controlled item(s) are at MIT or are in possession of MIT personnel. MIT complies with all U.S. export control laws.

## 2. Controlled Access – Identifying Authorized Personnel

To avoid violations of U.S. export control laws, access to the export-controlled item(s) are restricted solely to the personnel named in this TCP. Sharing technology, technical data, or source code with unauthorized persons is a violation of U.S. export control law and can result in fines up to one million dollars per violation and up to 20 years imprisonment. MIT, the Responsible Individual, and the person who caused the violation all can be held responsible. Over time, additional personnel can be added to the TCP by submitting an addendum to the Export Control Officer. (Add more rows if needed)

**Authorized Personnel**

List all personnel who will have access to export-controlled items, including the RI. The RI is responsible for training all personnel in the security procedures of this TCP. The RI and all other personnel with access to the item(s) must complete CITI Export Control training before the TCP is approved. Date active is the date added to the TCP.

To add or remove personnel after the TCP is initially approved, please contact the Export Control Officer.

1. **Authorized Personnel: U.S. Citizens**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | MIT Title | Role on Project | Date Active | Trained on TCP by RI | Trained in CITI |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**2. Authorized Personnel: U.S. Permanent Residents**In addition to the information above, provide the nationality for all authorized personnel who are not U.S. Citizens.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | MIT Title | Role on Project | Date Active | Trained on TCP by RI | Trained in CITI | Nationality |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**3. Authorized Personnel: Non-U.S. Permanent Residents**In addition to the information above, provide the visa status for all authorized personnel who are not U.S. permanent residents.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | MIT Title | Role on Project | Date Active | Trained on TCP by RI | Trained in CITI | Nationality | Visa Status |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**4. Non-Disclosure Agreement** (for ITAR technical data only)

Bona fide full-time employees who are not permanent U.S. residents and request access to ITAR technical data must sign an MIT Non-disclosure Agreement (NDA). Contact the Export Control Officer for more information**.**

|  |  |
| --- | --- |
| Name | Date NDA Signed |
|  |  |
|  |  |

## Responsibilities of the Responsible Individual (RI)

* The Responsible Individual (RI) is legally responsible for the security of the export-controlled item(s) in this TCP and for compliance with all applicable U.S. export control laws.
* The RI must inform MIT’s Export Control Officer of changes to this TCP.
* The RI must inform MIT’s Export Control Officer of all personnel access updates.
* The RI must train in security procedures, all faculty, staff and students with access to the export-controlled item(s). Such persons should complete the MIT CITI Export Control Training module.
* The RI is responsible to respond to the Export Control Officer Annual Review of TCPs.
* The RI must inform MIT’s Export Control Officer when the controlled item has been expended, removed from MIT’s campus, or no longer needed.
* The RI must inform MIT’s Export Control Officer of any breach in plan and will be **liable** for export control violations associated with the item(s) in this TCP.
* The RI must inform the MIT Export Control Officer if s/he can no longer perform his/her duties (e.g. when on sabbatical).

**The Responsible Individual will report any breach of this plan to the Export Control Officer immediately upon discovery of the breach via email at exportcontrolhelp@mit.edu or phone at (978) 590-0974.**

**Responsible Individual**

|  |  |
| --- | --- |
| Is the Responsible Individual: | U.S. Citizen  U.S. permanent resident |

## Project/Award Description

Describe your research and why you need export-controlled item(s).

**Research Project/Award**

|  |  |
| --- | --- |
| Project /Award Name |  |
| Research Sponsor |  |
| Award Number |  |
| Description |  |
| Expected Duration |  |
| Where will the research be conducted? |  |
| Why does the project require export-controlled item(s)? |  |
| Are there reasonable alternatives to using export-controlled item(s)? Please explain. |  |
| Can the research be conducted without the export-controlled items(s)? | Yes  No |

## Export-Controlled Item(s)

Describe the export-controlled item(s).

**Item(s)**

|  |  |
| --- | --- |
| Item Name |  |
| Item Type: | Technical data  Technology  Software  Tangible item |
| Item Make/Model |  |

## Procurement

Describe how the RI will come into possession of the item(s.)

**Removing Item(s) from MIT Possession**

|  |  |
| --- | --- |
| How will the RI acquire the item? | Purchase  Loan  License |
| From where or from whom will the RI acquire the item (i.e. who is the supplier)? |  |
| If the item is data, is there a Data Use Agreement (DUA)? | Yes  No |
| If the item is data, is it Controlled Unclassified Information (CUI)? | Yes  No |
| Will the RI obtain this item as part of a Sponsored Research Agreement (SRA)? | Yes  No |
| Is there a purchase order for this item? If yes, what is the number? | Yes  PO #       No |
| Is procurement involved in obtaining the item? | Yes  No |

## Preventing Unauthorized Access

Describe the RI’s plan to prevent access to the export-controlled item(s) by unauthorized personnel (use space below or attach separately). If item(s) are data, software, or require electronic access, read [Appendix 1](#APP2) and contact MIT Cybersecurity Officer at [researchcybersecurity@mit.edu](mailto:researchcybersecurity@mit.edu) to assist in your security plan.

|  |
| --- |
| **What measures will the RI take to protect the item(s) from *unauthorized physical access*?**  Use as much space as necessary to provide a detailed plan. |
|  |

|  |
| --- |
| **What measures will the RI take to protect the item(s) from *unauthorized electronic access*?**  Use as much space as necessary to provide a detailed plan. |
|  |

**Note: If there is a change in usual location of the controlled item, please inform MIT Export Control; it requires a documented modification to the TCP.**

## Removal Plan

Describe the RI’s plan to remove the export-controlled item(s) from MIT’s possession. If item(s) are data, software, see [Appendix 1](#APP2) and contact MIT Cybersecurity Officer at [researchcybersecurity@mit.edu](mailto:researchcybersecurity@mit.edu) to assist in your security plan. See [Appendix 2](#APP3) for removing or destroying tangible items.

**Removing Item(s) from MIT Possession**

|  |  |
| --- | --- |
| How will the RI dispose of **hard-copy restricted material** from MIT’s possession when the project ends? |  |
| How will the RI remove **tangible item(s)** from MIT’s possession when the project ends? |  |

## Compliance Procedures

The Export Control Officer may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the Export Control Officer. The Export Control Officer will conduct annual reviews of all active TCPs for update and/or closure.

## TCP Authorization

This represents my request for an exception to the open research policy, and my commitment to ensure compliance with U.S. export control laws. I understand and agree to follow the procedures outlined in the TCP. I will consult with MIT’s Export Control Officer in the case of any uncertainties. I understand that I could be held **personally liable** if I unlawfully disclose export-controlled information to unauthorized persons.

Name: Date

Title:

Department:

**Department, Lab, or Center Head Signature**

Name: Date

Professor, Department Head

Department:

**Research Compliance Team Signature**

I accept this Technology Control Plan on behalf of the Institute.

Gregory Moffatt Date

Chief Research Compliance Officer

Office of the Vice President for Research

## Appendix 1 Guidelines for Accessing, Storing, Destroying, and Transmitting Export-Controlled Data at MIT

ITAR or EAR export-controlled information (referred to as Controlled Information in this document) that is stored at MIT should be managed in accordance with the following guidelines.

1. **Contact Research Cybersecurity**

Contact Research Security at [researchcybersecurity@mit.edu](mailto:researchcybersecurity@mit.edu) to consult on plans. Research Security provides the following services at no cost:

* Security software, including Sophos Antivirus and CrowdStrike Falcon (please contact [researchcybersecurity@mit.edu](mailto:researchcybersecurity@mit.edu) ), a cloud-based anti-malware platform monitored in real-time by trained security professionals.
* Membership in the IS&T-managed active directory domain, providing Kerberos authentication, regular security patches, and two-factor authentication where appropriate.

1. **Data Access**

* Controlled Information should not be accessed from shared or public computers such as kiosk computers in libraries, hotels, and business centers.
* Systems with access to Controlled Information should be well-maintained (patched/updated regularly) and run security software to detection malware or compromise.
* Access to Controlled Information should be provided to individuals on a “need to know” basis and in accordance with rules governing who is restricted from access (nationality, etc.).
* Protect Controlled Information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control. Please refer to [infoprotect.mit.edu](https://infoprotect.mit.edu/high-risk-data-classifications/) for the full range of protection for high-risk data.

1. **Data Storage**

* Controlled Information must be stored on Institute-owned devices and access controlled with individually assigned accounts requiring username/password or user certificates. Two-factor authentication should be enforced for access to highly sensitive data.
* All Controlled Information must be encrypted if stored on laptops, mobile devices (smartphones, tablets), or removable media (USB drives, CD/DVD). Cloud-based storage platforms, such as Dropbox or OneDrive, may be acceptable for some forms of Controlled Information with Export Control Officer approval.
* MITnet is an open network and frequently targeted by attackers. It is essential that systems storing Controlled Information be well-maintained (patched/updated regularly) and properly secured against unauthorized access. If your team lacks this expertise, please contact [researchcybersecurity@mit.edu](mailto:researchcybersecurity@mit.edu) for assistance.

1. **Data Destruction**

Electronic media holding Controlled Information should be wiped in accordance with NIST 800–88, Guidelines for Media Sanitization. If destruction of media is desired, IS&T has relationships with several data destruction vendors and can offer assistance. Please contact servicedesk@mit.edu for more information.

1. **Data Transmission**

Transmission of Controlled Information should be encrypted. If you are receiving CUI and you haven’t already discussed with MIT Export Control, please contact the Export Control Officer.

Transmission of Controlled Information via voice or fax is permissible only when there is reasonable assurance that access is limited to authorized persons.

**Notify MIT Export Control when you remove export-controlled data from MIT’s possession.**

## Appendix 2 Removing Export-Controlled Tangible Items from MIT

1. If you own a broken item and want to destroy it, contact MIT Property to confirm title and ownership and obtain disposal instructions to ensure government standards for disposal of restricted items are met.
2. If you own a functional item and do not want it, you can:

* Sell: Contact MIT Property to find a buyer through the use of secondary market equipment brokers. Only MIT titled equipment can be sold.
* Donate Outside MIT: Contact MIT Property to confirm title and ownership prior to donation.
* Transfer within MIT: Forward the MIT equipment tag number along with new Responsible Individual and new location to MIT Property.

1. If item was bought with sponsor (contract) funds, you can:
   * Return to sponsor: Notify MIT Property and forward the MIT Asset Tag information. If sponsor does not want it back, contact MIT Property for surplus equipment options.
   * Dispose it: Contact MIT Property to deactivate the equipment record in their database. They will assist with the most cost-effective way to handle disposal.
2. If item was on formal loan, contact MIT Property.

**MIT Property Office MIT Export Control**

NE49-3000 NE18-901

617-253-2776 (978) 590-0974

[property@mit.edu](mailto:property@mit.edu) [exportcontrolhelp@mit.edu](mailto:exportcontrolhelp@mit.edu)

**Notify MIT Export Control when you remove export-controlled items from campus.**

1. If applicable [↑](#footnote-ref-1)
2. State the number of years, months, whether it is open-ended, or if this field is not applicable. [↑](#footnote-ref-2)