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

## Technology Control Plan Summary

|  |  |
| --- | --- |
| Date |  |

### Responsible Individual (RI)

|  |  |
| --- | --- |
| RI Name |  |
| RI Title |  |
| RI Department, Lab, or Center |  |

### Project

|  |  |
| --- | --- |
| Project Title[[1]](#footnote-1) |  |
| Expected Project Duration[[2]](#footnote-2)  |  |

### Export-Controlled Item(s)

|  |  |
| --- | --- |
| Item Name |  |
| Item Type[[3]](#footnote-3) |  |
| Controlling Agency[[4]](#footnote-4) |  |
| Item Classification[[5]](#footnote-5) |  |

## MIT Policy

[MIT Policy 14.2](https://policies.mit.edu/policies-procedures/140-research-policies-and-public-and-private-support/142-open-research-and-free) does not allow research on campus that restricts the participation of foreign faculty, students, and scholars unless the work is crucially important to MIT's educational mission and the exception is demonstrably necessary for the national good. MIT prohibits export-controlled items (e.g., material, information, data, etc.) on campus unless the Vice President for Research approves a Technology Control Plan (TCP). Each TCP must identify a Responsible Individual (RI). The RI is an MIT faculty or staff member who is legally responsible for ensuring compliance with U.S. export control laws while the export-controlled item(s) are at MIT or are in possession by MIT personnel. MIT personnel includes MIT faculty, staff, students, and their agents. MIT complies with all U.S. export control laws and regulations including the [Export Administration Regulations (EAR)](https://www.bis.gov/regulations), [International Traffic in Arms Regulations (ITAR)](https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987), [Department of Energy Regulations 10 CFR Part 810](https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title10/10cfr810_main_02.tpl), and [Office of Foreign Assets Control (OFAC)](https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx).

All faculty, staff, and students with access to export-controlled item(s) must be trained in the security procedures of this TCP and are highly encouraged to complete [MIT CITI Export Control Training](https://www.citiprogram.org/members/index.cfm?pageID=50).

## Authorized Personnel (See [APPENDIX 1](#APP1))

To avoid violations of U.S. export control laws, access to the export-controlled item(s) are restricted solely to the personnel named in [Appendix 1](#APP1) of 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. Additional personnel can be added to the TCP by submitting an addendum to the Export Control Officer.

## 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 will be **personally liable** for export control violations associated with the item(s) in this TCP. The RI must inform MIT’s Export Control Officer of changes to this TCP in writing. This includes changes to personnel with access to the item(s) and when items are uninstalled, destroyed, or otherwise removed from MIT’s campus and control.

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 (617) 253-2762.

The Responsible Individual is responsible for conducting annual self-evaluations to assure continued compliance with this Plan, reporting any findings to the Export Control Officer, Janet C. Johnston, jcjohnst@mit.edu, 617 253 2762, or to the Chief Research Compliance Officer, Greg Moffatt, GTM@mit.edu,  617-253-9584.

Non-U.S. residents who are bona fide full-time employees of MIT must sign a Non-Disclosure Agreement (NDA) if receiving access to technical data controlled under the [International Traffic in Arms Regulations (ITAR)](https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987).

### Responsible Individual

|  |  |
| --- | --- |
| Is the Responsible Individual a U.S. citizen or a U.S. permanent resident? |  |
| If the RI is not a U.S. citizen or a U.S. permanent resident and the item(s) is technical data controlled by ITAR, has the RI signed an MIT Nondisclosure Agreement? |  |

## Project/Award Description

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

### Research Project/Award

|  |  |
| --- | --- |
| Project/Award Name |  |
| Sponsor |  |
| 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)? |  |

## Export-Controlled Item(s)

*Describe the export-controlled item(s).*

### Item(s)

|  |  |
| --- | --- |
| Item Name |  |
| Item description (e.g., data, software, tangible) |  |
| Item Make/Model |  |

## Procurement

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

### Plan for Obtaining Item(s)

|  |  |
| --- | --- |
| How will the RI acquire the item (e.g., 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)? |  |
| If the item is data, is it Controlled Unclassified Information (CUI)? |  |
| Will the RI obtain this item as part of a Sponsored Research Agreement (SRA)?  |  |
| Is there a purchase order for this item? If yes, what is the number? |  |
| Is procurement involved in obtaining the item? |  |

## 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 2*](#APP2) *and contact MIT IS&T Information Security Officer* *Jessica Murray* *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.* |
|  |

## 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 2*](#APP2) *and contact MIT IS&T Information Security Officer* *Jessica Murray* *to assist in your security plan. See* [*Appendix 3*](#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?  |  |
| How will the RI remove electronic 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 or the Empowered Official for export control*.* 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.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| NameTitleDepartment |  | Date |

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

I am aware that use of this restricted information represents an exception to MIT research policy, and endorse the exception and the suitability of the Technology Control Plan.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| NameProfessor, Department HeadDepartment |  | Date |

**Office of Research Compliance Signature**

I accept this Technology Control Plan on behalf of the Institute

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Greg MoffattChief Research Compliance OfficerOffice of the Vice President for Research |  | Date |

## Appendix 1Authorized Personnel

*List the personnel who will have access to the item(s), 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. Date inactive is the date removed from the TCP.*

*To add or remove personnel after the TCP is initially approved, use “track changes” to update the information. Submit Appendix 1 to the* *Export Control Officer**.*

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **MIT Title** | **Role on Project** | **Date Active** | **Date Inactive** | **Trained on TCP** | **Trained in CITI** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **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** | **Date Inactive** | **Trained on TCP** | **Trained in CITI** | **Nationality** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. **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** | **Date Inactive** | **Trained on TCP** | **Trained in CITI** | **Nationality** | **Visa Status** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

1. **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** |
|  |  |
|  |  |

## Appendix 2 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 IS&T**

Contact IS&T at security@mit.edu to secure the storage, access, and destruction of Controlled Information. IS&T provides the following services at no cost:

* Security software, including Sophos Antivirus and Crowdstrike Falcon, 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.

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 Office 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 security@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 security@mit.edu for more information.

1. **Data Transmission**

Transmission of Controlled Information should be encrypted. Access to Controlled Information over WiFi must be encrypted using VPN or by using an encrypted wireless network (“MIT SECURE” or “eduroam”). If Controlled Information is sent via email, message encryption – such as PGP or S/MIME – should be used to encrypt message content. If message encryption is not possible, encryption of attachment data – such as using native Microsoft Office encryption - is permissible.

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 3Removing 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 was on formal loan**,** contact MIT Property.

**MIT Property Office**

NE49-3000

617-253-2776

property@mit.edu

**MIT Export Control Office**

NE18-901

617-253-2762

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)
3. Is the item technical data, technology, software, or a tangible item? (select one) [↑](#footnote-ref-3)
4. Which U.S. agency regulates the use of this item (e.g., State, Commerce, Treasury, Energy, etc.)? [↑](#footnote-ref-4)
5. What is the item classification (e.g., ECCN, ITAR category)? [↑](#footnote-ref-5)