Boston University BU Research Compliance

TECHNOLOGY CONTROL PLAN TEMPLATE

Developed and Approved by

Marie Hladikova, Export Control Director

Boston University, Office of Research Compliance

Date: _____

Revised March, 2015

1) COMMITMENT

Boston University is committed to compliance with all export control laws and regulations. Link here for University's Export Control Policy. The Office of Research Compliance is responsible for implementation of technology control plans as applicable. The Empowered Officials for export controls are Kathryn Mellouk, Associate Vice President for Research Compliance and Marie Hladikova, Export Control Director. Marie Hladikova is the main contact for export control issues. The individual responsible for and committed to ensuring compliance with this TCP is

……

2) SCOPE

The procedures contained in this plan apply to all individuals involved in

…….…….. project at Boston University.

Export of controlled data/items abroad or to a foreign national who is a visitor, researcher, student or employee of Boston University may require an export license by the Directorate of Defense Trade Controls.

3) PURPOSE

The purpose of this plan is to inform the Boston University researchers, employees, Students and visitors of the controls that are in place to protect inadvertent release or export of controlled data/services under the International Traffic in Arms Regulations.

4) PROJECT DESCRIPTION

5) EXPORT CONTROL CLASSIFICATION

Classification determinations will be managed by the Export Control Director using OCR Services.

6) EXPORT REGULATIONS AND REQUIREMENTS

ITAR OVERVIEW

The International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130, govern the export, re-export and import of classified and unclassified defense articles, defense services, and related technical data from the United States, abroad, and/or to any foreign person, whether located in the United States or abroad. The ITAR controls not only end items, such as radar and communications systems, military encryption and associated equipment, but also the parts and components that are incorporated into the end item. Certain non-military items are also controlled.

With rare exceptions, if an item contains any components that are controlled under the ITAR, the entire item is controlled under the ITAR. For example, a commercial radio that would normally not be controlled under the ITAR becomes a controlled defense article if it contains an ITAR-controlled microchip. The Directorate of Defense Trade Controls (DDTC) administers and enforces the regulations. An article or service may be designated or determined in the future to be a defense article or defense service if it:

- Is specifically designed, developed, configured, adapted, or modified for a military application
- Does not have predominant civil applications
- Does not have performance equivalent (defined by form, fit, and function) to those of an article or service used for civil applications
- Is specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability such that control under this subchapter is necessary

The intended use of the article or service after its export (i.e., for a military or civilian purpose) is not relevant in determining whether the article or service is subject to the controls of this subchapter. Any item covered by the U.S. Munitions List (USML) must be within the categories of the U.S. Munitions List.

ITAR DEFINITIONS

Defense Article

Means any item or technical data that is specifically designed, developed, configured, adapted, or modified for a military, missile, satellite, or other controlled use listed on the USML. Defense article also includes models, mock-ups, or other items that reveal technical data relating to items designated in the USML.

Technical Data

Means any information which is required for the design, development, assembly, production, operation, repair, testing, maintenance, or modification of a defense article. Technical data may include drawings or assembly instructions, operations and maintenance manuals, and email or telephone exchanges where such information is discussed. However, technical data does not include general scientific, mathematical, or engineering principles commonly taught in universities, information present in the public domain, general system descriptions, or basic marketing information on function or purpose.

Under ITAR certain data that are considered as being in "public domain" are exempted (provided that the publication of the data was authorized). Exercise diligence when using information that you find on the internet. It occasionally happens that individuals inadvertently place ITAR information in the public domain without the required approval. If you find data that would not normally be published, contact the University Export Control Director to provide assistance whether you can use it without a license in your research.

Public domain means information that is published and generally accessible or available to the public:

- Through sales at newsstands and bookstores
- Through subscriptions available without restriction to any individual who desires to obtain or purchase the published information
- Through second class mailing privileges granted by the U.S. Government
- At libraries open to the public or from which the public can obtain documents
- Through patents available at any patent office
- Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States
- Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency
- Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community.

Defense Service

Means providing assistance—including training—to a foreign person in the United States or abroad in the design, manufacture, repair, or operation of a defense article, as well as providing technical data to foreign persons. Defense services also

include informal collaboration, conversations, or interchanges concerning technical data.

U.S. Person

U.S. person means a person who is U.S. citizen, or a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state, or local) entity.

DEFINITION OF THE EXPORT UNDER THE ITAR

Export means sending or taking a defense article out of the United States in any manner, except by mere travel outside of the United States by person whose personal knowledge includes technical data; or transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the US Munitions List, whether in the United States or abroad; or disclosing (including oral and visual disclosure) or transferring technical data to a foreign person whether in the United States or abroad; or performing defense services on behalf of, or for the benefit of, a foreign person, whether in the Unites States or abroad.

AUTHORIZATION TO EXPORT

Any export or transfer of ITAR article, technical data or software to foreign national at or outside of Boston University is subject to an authorization by the Directorate of Defense Trade Controls. Exemptions must be approved by the University Export Control Director prior to the export/transfer. In addition, travel abroad with technical data (on a laptop, in an email, presentation or research paper), software or hardware is subject to ITAR authorization and must be authorized by the Directorate of Defense Trade Controls. Exemptions must be approved by the University Export Control Director prior to the travel.

Boston University is registered with the Directorate of Defense Trade Controls and as such, we have the ability to submit license applications and take advantage of certain exemptions.

EMBARGOED COUNTRIES UNDER THE ITAR

Currently, the list of countries includes: Afghanistan, Belarus, Burma, China (PR), Côte d'Ivoire, Cuba, Cyprus, Democratic Republic of the Congo, Eritrea, Fiji, Republic of Guinea, Haiti, Iran, Iraq, Kyrgyzstan, Lebanon, Liberia, Libya, North Korea, Pakistan, Somalia, Sri Lanka, Sudan, Syria, Venezuela, Vietnam, and Zimbabwe.

ITAR Prohibitions: No ITAR exports may be made either under a license or license exemption to countries proscribed in 22 C.F.R. § 126.1. Moreover, no foreign

students, scholars, collaborators, companies from these countries shall have access to ITAR controlled research, technical data, or services. Note: These lists are regularly updated. It is essential that the list be consulted prior to any transaction. For the most updated list please refer to:
http://www.pmddtc.state.gov/embargoed_countries/index.html.

The University is under a mandatory disclosure requirement for any disclosures to these countries.

RECORD KEEPING

All records related to export or import shipments, research projects, licenses, agreements and/or license exceptions must be kept on file for five years after the shipment/project is finalized or the export license expired whichever is longer.

IMPORTING

There are two primary regimes that govern the import of ITAR articles. Temporary import, ITAR hardware that was previously exported from the U.S. is subject to DDTC's jurisdiction and authorization.

The permanent import of defense articles listed on the U.S. Munitions Import List requires an import license from the Bureau of Alcohol, Tobacco, Firearms and Explosives and importers must be registered with the ATF. The U.S. Munitions Import List is not as comprehensive as the USML and doesn't include all ITAR items so it is important to carefully review its applicability prior to the import. It is located at 27 CFR §447.21. This list mostly governs critical military items and few space related items and equipment.

7) PROJECT SPONSORS AND VENDORS

Sponsors:

Vendors:

Vendors developing custom components or software require vetting prior to their involvement in ITAR research. Before you provide any ITAR controlled data or job order to a vendor in the United States, confirm the following:

1. The vendor is eligible to fulfill ITAR orders; and
2. The vendor employs only U.S. Persons or will develop a technology control plan to ensure that only U.S. Persons have access to the information that Boston University provides to the vendor to fulfill an order; and
3. The vendor signs the vendor verification letter on the following page.

Collaborations with vendors outside of the United States require an ITAR authorization.

VENDOR VERIFICATION LETTER

Vendor's Address

Dear ……

The purpose of this letter is to inform you that the Boston University project

……. is subject to the International Traffic in Arms Regulations (ITAR) as administered by the Directorate of Defense Trade Control. As such, we ask you to certify to us that you are in compliance with 22 CFR Parts 120-130.

The minimum requirements of ITAR compliance include registration with the Directorate of Defense Trade and establishment of procedures to prevent the export/ release of information, data, hardware, software or services abroad or to non U.S. Persons in the United States. Additionally, each entity working with ITAR controlled data must ensure that such data is not released to foreign nationals whether in the United States or abroad as defined in 22 CFR section 120.16 without the authorization from the Directorate of Defense Trade Controls.

We ask you to certify, by signing this document, that you are compliant with the International Traffic in Arms Regulations and eligible to fulfill this order.

If you have any questions regarding this request, feel free to contact our University Export Control Director, Marie Hladikova at 617-353-6753 or via email at mhladiko@bu.edu.

……
Name, Title, Company Name

……..
Signature

……..
Date

8) PERSONNEL SCREENING

All participants will be screened via the International Student and Scholars Office (ISSO) prior to their involvement and only eligible individuals will be allowed to work on controlled research.

The list of individuals who are eligible to participate in the research is included in the Project Employee List.

Boston University uses OCR Services Software to screen against the Denied Parties Lists and the Export Control Director will manage student/scholar screening.

Principal Investigator is required to report any new student/faculty participants to the Export Control Director prior to their involvement in the project.

PROJECT EMPLOYEE LIST

Name	U.S. Person Yes/No	BUID	Email	License/ Exemption	Training	Forms Completed

9) Technology Control Plan Acknowledgment

All individuals working on the project shall sign a statement that acknowledges that controlled information will not be disclosed, exported or transmitted to any foreign national or foreign country unless the respective federal government agency authorizes such a disclosure and the receiving party is appropriately screened to receive export controlled data. This form will be signed prior to their involvement in the project.

The team will use the TCP Acknowledgement Form tor that purpose.

Students will sign the Acknowledgment Form for FERPA purposes.

ACKWNOWLEDGMENT OF TECHNOLOGY CONTROL PLAN
U. S. PERSON

This is to acknowledge that I, …….,

understand that any technical data related to *the ……. project* covered by the U.S. Munitions List to which I have access as a U.S. Person and disclosed to me in the course of my research and/or employment at Boston University is subject to the International Traffic in Arms Regulations.

As such, none of the technical data, software, hardware or services can be exported or transferred to foreign national or abroad without an authorization by the Directorate of Defense Trade Controls. I further agree that I will not travel abroad with technical data, hardware or software without the authorization by the Directorate of Defense Trace Controls.

I acknowledge and understand that should I inadvertently receive defense articles or technical data related to defense articles for which I do not have an authorized access; I will report such unauthorized access to the University Export Control Director or the Associate Vice President for Research Compliance within 24 hours of such receipt. Additionally, I will notify the Principal Investigator.

I acknowledge and understand that violations of the International Traffic in Arms Regulations carry significant penalties and imprisonment and I can be held personally responsible for unlawful transfer or export of ITAR articles and data.

I acknowledge that I received this Technology Control Plan in advance, read it and discussed the procedures

With ……..…… I understand the procedures and agree to comply with its requirements. I also understand that this commitment extends beyond my employment/tenure with Boston University.

……..
DATE

……..
SIGNATURE

……..
EMPOWERED OFFICIAL SIGNATURE

ACKNOWLEDGMENT OF TECHNOLOGY CONTROL PLAN
FOREIGN PERSON

This is to acknowledge that I, ……., understand that any technical data related to *the ……. project* covered by the U.S. Munitions List to which I have access per authorization by the Directorate of Defense Trade Controls License/Exemption …… and disclosed to me in the course of my research and/or employment at Boston University is subject to the International Traffic in Arms Regulations.

As such, none of the technical data, software or hardware can be exported/transferred to foreign national or abroad without an authorization by the Directorate of Defense Trade Controls. I further agree that I will not travel abroad with technical data, hardware or software without the authorization by the Directorate of Defense Trace Controls.

I acknowledge and understand that should I inadvertently receive defense articles or technical data related to defense articles for which I do not have an authorized access; I will report such unauthorized access to the University Export Control Director or the Associate Vice President for Research Compliance within 24 hours of such receipt. Additionally, I will notify the Principal Investigator.

I acknowledge and understand that violations of the International Traffic in Arms Regulations carry significant penalties and imprisonment and I can be held personally responsible for unlawful transfer or export of ITAR articles and data.

I acknowledge that I received this Technology Control Plan, read it and discussed the

procedures with ……..……. and that I understand the procedures and agree to comply with its requirements. I also understand that this commitment extends beyond my employment/tenure with Boston University.

…….
DATE

……..
SIGNATURE

…….
EMPOWERED OFFICIAL SIGNATURE

AUTHORIZATION FORM

Boston University
Boston, Massachusetts 02215

Name of Student: _____ BU ID: _____

Project / Program / Course:

I, the undersigned, hereby authorize Boston University to release information concerning my participation in the project, program or course identified above or related work to governmental authorities or regulators as necessary to meet the University's obligations under export control laws.

I understand further that (1) I have the right not to consent to the release of my education or financial records; (2) I have the right to receive a copy of such records upon request; and (3) that this consent shall remain in effect until revoked by me, in writing, and delivered to Boston University, but that any such revocation shall not affect disclosures previously made by Boston University prior to the receipt of any such written revocation.

_____ _____

Student's Signature Date

_____

Signature of Parent or Guardian
if student is under 18

THIS INFORMATION IS RELEASED SUBJECT TO THE CONFIDENTIALITY PROVISIONS OF APPROPRIATE STATE AND FEDERAL LAWS AND REGULATIONS WHICH PROHIBIT ANY FURTHER DISCLOSURE OF THIS INFORMATION WITHOUT THE SPECIFIC WRITTEN CONSENT OF THE PERSON TO WHOM IT PERTAINS, OR AS OTHERWISE PERMITTED BY SUCH REGULATIONS.

10) APPLICABLE LICENSES AND EXEMPTIONS

ITAR licenses and exemptions will be managed by the Export Control Director using OCR Services.

11) PHYSICAL SECURITY

Location

Laboratory where ITAR controlled research takes place will remain under lock and key or swipe card access at all times.

All ITAR controlled materials, samples, measurements; data will remain in the room at all times. In addition, the room will be the physical location of all the ITAR controlled IT assets such as laptops, PC's, etc.

If an ITAR controlled device, hardware, component, software or has to be moved out of the lab for any reason (upgrade, repair, move to a new location etc.) the University Export Control Director will be notified in writing or by email 72 hours in advance and the team will wait for a confirmation that the item can be removed to another research laboratory.

Access Controls

All foreign nationals must be pre-authorized by the University Export Control Director prior to the visit to the ITAR controlled laboratory. The Principal Investigator or other personnel working on the project will inform the University Export Control Director if a visit by foreign national is desired so that appropriate security procedures can be implemented to prevent unauthorized access to ITAR data, hardware or software by the foreign visitor.

No foreign visitor may access the laboratory when the research takes place without proper licensing authorization by the Directorate of Defense Trade Controls.

All other U.S. Person visitors will be escorted in the laboratory at all times by one of the persons authorized to work on the project and will not be given access to ITAR controlled data.

Only individuals that have been authorized by the Principal Investigator and the University Export Control Director will have access to the laboratory where controlled research takes place, unless they are University Officials and Administrators with a valid reason for access such as a compliance audit.

Prior to any visit by maintenance personnel or anyone coming to the research lab to conduct repair, equipment replacement or any other valid reason, the University Export Control Director must be notified ahead of time to assess what security procedures must be in place to prevent incidental access to ITAR data.

In the event of an accident beyond the reasonable expectation which may require emergency response by law enforcement or medical professionals, the University Export Control Director will be notified as soon as practical.

Physical Security for Export Controlled Data and Technical Information

Document Control

All documents that are subject to the ITAR will be labeled with an appropriate language such as “ITAR Controlled.”

All documents containing controlled information or data should be shredded when it is no longer needed. Only U.S. persons are allowed to dispose controlled information.

All documents that contain controlled information or data should be locked in secure lockable cabinets to prevent unauthorized access. The Principal Investigator will ensure that only individuals that have been pre-screened have access to the information. If any information is stored on shared network, the area of the network will be secured with a password that will be given to individuals that have been approved to have access to ITAR information.

All research labs will employ a “clean desk” procedure which means that no controlled information will be left unattended. Computer screen will be closed when the researcher is not at his or her desk. Blueprints, technical data and information will be securely locked in a cabinet or a desk when it is not used to prevent unauthorized access.

Copy machine usage – no copies of ITAR data will be left unattended on a copy machine.

Fax usage – fax dissemination of controlled information should be avoided if at all possible and if a fax machine has to be used, the person transmitting the information should ensure that only approved individual will receive the data.

Printers – all controlled information should be immediately picked up from the printers to prevent unauthorized access.

Website – no ITAR controlled data/information shall be posted on any public website (including personal Facebook, MySpace and other social media sites) without prior written approval of the Principal Investigator and the University Export Control Director.

12) INFORMATION SECURITY

(Project specific IT&S controls will be included in this section)

The Boston University System rules require all researchers to ensure that sensitive digital research data is appropriately protected. ITAR controlled data have been labeled as “restricted use” and has to be protected in accordance to Boston University Data Security policy: http://www.bu.edu/tech/about/policies/info-security/1-2-a-data-classification-guide/

In accordance with those rules, Boston University provides guidance on procedures for Protecting Sensitive Digital Research Data found at http://www.bu.edu/tech/policies/info-security/ that will be followed for protection of controlled information under this TCP.

All of the following data/documents be restricted from disclosure to foreign nationals and shall be protected as Restricted Use data:

1) Critical Program Information (designated as Critical Program Information by the Department of Defense and its agencies; NASA; Department of Homeland Security; Department of Energy; NOAA or any other agency)
2) Designated for withholding from public release under DOD Directive 5400.07 (Freedom of Information Act)
3) Containing designations indicating access control (e.g., For Official Use Only, Sensitive but Unclassified, Limited Distribution, Distribution to Department of Defense and its Contractors Only, Proprietary, Originator Controlled, Law Enforcement Sensitive)
4) ITAR Technical Data received from the sponsor or generated during the effort.

Technical data and reports, computer software covered under DOD Directive 5230.24, Distribution Statements on Technical Documents, and DOD Directive 5230.25 Withholding of Unclassified Technical Data from Public Disclosure.

ITAR controlled data will not be stored on the cloud unless the University Export Control Director can confirm with the cloud service provider that the cloud is an ITAR secure environment.

It is recommended that researchers use Boston University enterprise encryption solution to secure ITAR controlled data on portable devices such as laptop, thumb drive, CD etc. http://www.bu.edu/tech/security/data-protection/drive-encryption/

Computers - when a computer has reached its usable life or is used for another project, the hard drive will be forensically erased or destroyed using University hard drive destruction services http://www.bu.edu/tech/security/data-protection/media-destruction/.

Communication

Voicemail – Voicemail shall not be used to transmit ITAR technical data to prevent unauthorized access. Voicemail should be used only to relay informational messages such as – scheduling meetings related to ITAR research, schedule visits etc.

Instant Messaging – Instant messaging shall not be used to transmit ITAR data and information.

Telephone – ITAR information can be transmitted via phone if previously authorized and if the other party on the call has been pre-screened and has been authorized to receive controlled information**.**

Teleconference/Netmeetings – ITAR information can be transmitted via netmeetings, provided that you pre-screened all of the parties on the call and have a password to protect unauthorized access.

Email - All individuals working on the ITAR controlled project will use BU exchange or secure email only. Emails containing ITAR information should be send only to individuals that are authorized to have access to the materials. BU Google Apps shall not be used to store, maintain or transmit export controlled information. All students participating in the project are required to use the exchange email service provided by IS&T. All students will follow the guidelines on IS&T's website and will obtain a secure email to transmit data: http://www.bu.edu/tech/accounts/special/datamotion-securemail/ To have a student moved to Exchange, submit a service request by hitting the Help icon anywhere on the IS&T web site.

All communication via email that contains ITAR/EAR data should have the following disclaimer: **"This email contains information/data that is controlled under the International Traffic in Arms Regulations (ITAR) and is intended for the recipient only. No unauthorized transfer/export/release/sale or other disposition of this information is permitted without an export license from the U.S. Department of State, Directorate of Defense Trade Controls. If you received this email in error, notify the sender identified in this email immediately."**

Online Activity - All individuals working on ITAR controlled research are prohibited form posting technical data or information online without prior authorization by the cognizant governmental agency and the University Export Control Director.

Conversations – Technical discussions related to controlled projects will be limited to the individuals identified in this Technology Control Plan. All project participants are

prohibited from discussing the technical details with individuals not authorized to work on the project.

Unsolicited Emails from Researchers at Other Departments or Institutions Outside of BU - Conduct due diligence in communicating with researchers from other departments or institutions seeking information about your research projects. You should always screen all requests for assistance or collaboration to ensure that these are legitimate requests. You may meet other researchers at meetings, conferences, seminars, other professional or social networking events. Sharing “too much” information about your research could not only jeopardize your research efforts, it could also violate export regulations.

13) CONFERENCE/MEETING PARTICIPATION

(This section will include a list of conferences and specific controls that will be in place to avoid disclosure of controlled information without an export license).

All papers, presentations or other materials including technical data must be approved prior to the public release by either the cognizant governmental agency or the Office of the Security Review.

14) INTERNATIONAL TRAVEL

(This section will include information related to international travel and PI plan to avoid taking export controlled information abroad without government approval).

Travel abroad with ITAR data, software or hardware requires an authorization by the Directorate of Defense Trade Controls. Principal Investigator will inform the University Export Control Director well in advance to secure ITAR authorizations or “clean” laptop in advance of the travel.

15) PUBLICATIONS

All publications that contain technical data must be submitted for publication approval to the cognizant governmental agency or the Office of the Security Review.

Graduate Thesis - Any graduate student that is working on ITAR controlled research to fulfill his or her thesis or dissertation requirement must be a US Person, otherwise, the University will be required to submit an export license for him/her to work on the controlled research.

If the student includes technical data in the graduate thesis, the publication must be approved by either the Cognizant Government Agency or Office of the Security Review prior to the publication as required by the regulations. It is important to recognize that the publication approval might be delayed and ultimately, publication of certain data may be denied for national security reasons. Moreover, the thesis advisory committee and defense committee must only include US Persons unless they have been authorized by a license or an exemption to participate on the committee.

Submit requests for publication approvals to the Export Control Director to coordinate these requests with the appropriate agency.

16) TRAINING AND AWARENESS

All project participants will receive ITAR training and will be briefed on the procedures set forth in this Technology Control Plan prior to their involvement. The Principal Investigator and University Export Control Director will maintain a training log for the participants.

TRAINING RECORD

TRAINING SESSION SUBJECT: ……..……

DATE: ……

PRESENTER: ……

DEPARTMENT: ……

NAME	SIGNATURE

17) COMPLIANCE ASSESSMENT

As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the Export Controls Director, Marie Hladikova at mhladiko@bu.edu (617-353-6753) or Kathryn Mellouk, Associate Vice President for Research Compliance at kateski@bu.edu (617-358-4730).

There are no restrictions on who may report an alleged incident. Anyone who has knowledge of such a deficiency is obligated to report it to BU officials. Under no circumstances will reporting such incidences in good faith be detrimental to an individual's standing within the organization. No person will be discriminated against or be subject to any reprisal for reporting, in good faith, a concern or violation of any export control regulations. Refer to Boston University's policy on reporting violations http://www.bu.edu/ethics/ethical-conduct.pdf

If the institutional officials determine that ITAR violation has occurred, the University will file a self-disclosure with the appropriate government agency.

18) PROJECT TERMINATION

Security measures will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminated when the information has been destroyed or determined to be no longer export-controlled. All documents related to the project will be kept on file 5 years after the termination of the project.