

**VIRGINIA
POLYTECHNIC
INSTITUTE AND STATE
UNIVERSITY**

**TECHNOLOGY
CONTROL PLAN**

Virginia Polytechnic Institute and State University
Technology Control Plan

I. Overview

As a public institution of higher education, Virginia Polytechnic Institute and State University (Virginia Tech) employs foreign nationals and hosts foreign visitors in connection with international exchange programs, international students, and other business agreements. It is the intent of Virginia Tech to employ foreign nationals and host international visitors, both long and short term, in the most welcoming manner possible while also assuring compliance with U.S. laws and regulations governing the export of certain commodities and technical data.

The U.S. Department of Commerce regulates certain dual-use technologies, materials, items, software, and technology by the Export Administration Regulations (EAR) and the U.S. Department of State controls the export of defense articles, the performance of defense services and defense article-related technical data through the International Traffic in Arms Regulations (ITAR). The Department of the Treasury regulates travel and business activities with sanctioned and embargoed countries through Office of Foreign Assets Control (OFAC) regulations.

Each employee is personally responsible for safeguarding export-controlled items, materials, software, technical data or technology as required by the above federal agencies from disclosure to foreign nationals or foreign persons (“foreign nationals”) without export license or other government approval if required. An export license or other government approval from the U.S. government is required before a foreign national may be given access to many items, materials, software, or technology controlled by either the U.S. Department of Commerce or the U.S. Department of State. No release of classified information (i.e. confidential, secret, top secret) is permitted to any person without the proper security level clearance and a documented “need to know” for that specific information.

Each employee is personally responsible for complying with travel to and business with countries, entities, and individuals sanctioned by the United States in regulations, laws, and executive orders enforced by OFAC.

Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations without export license or other government approval. Sponsored project agreements containing export controlled items, materials, software, or technology may require that project personnel formally request and obtain prior government approval before the release of a publication or presentation. These requests shall be made in compliance with, and within the time frame stated in the sponsored project agreement. If no time frame is stated in the project agreement, three to six months may need to be anticipated for approval to be received from the contracting officer. Public release of information shall not occur until permission or other government approval is received by U.S. Department of State, Office of Defense Trade Controls, (ODTC), or U.S. Department of Commerce, Bureau of Industry and Security (BIS).

Virginia Polytechnic Institute and State University
Technology Control Plan

II. Purpose

The purpose of this Technology Control Plan (TCP) is to delineate the controls necessary to ensure that the transfer of export controlled items, software, or technology, classified information or other unclassified but restricted data (e.g., Sensitive, NOFORN, Naval Nuclear Power Information) that is not to be conveyed in any manner to foreign national visitors, employees, and students beyond that which is approved for export by a license or other approval from the appropriate U.S. federal agency, or which is authorized to an individual possessing the required security classification and “need to know.”

III. Authority

The National Industry Security Program Operating Manual (NISPOM) 10-509 requires: “A Technology Control Plan is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the Cognizant Security Agency (CSA) determines that procedures already in place at the contractor’s facility are adequate. The TCP shall contain procedures to control access for all export-controlled information.”

International Traffic in Arms Regulations (ITAR) 22CFR §126.13 (c) also encourages use of a Technology Control Plan (TCP): “In cases when foreign nationals are employed at or assigned to security-cleared facilities, provision by the applicant of a Technology Control Plan (available from the Defense Investigative Service) will facilitate processing.”

IV. Existing Policies and Procedures

This TCP requires Virginia Tech adherence to the NISPOM. Regarding the handling of classified information reference is made to Virginia Tech’s agreement with the U.S. Department of Defense document dated October 16, 1970. These documents, including Virginia Tech’s Office of Sponsored Programs policy OSP-29-05 “Management of Export Controlled Sponsored Projects,” shall be considered a part of this TCP, by reference.

V. Definitions

A. Controlled Technical Data

Controlled technical data, are defined as follows (22 CFR §120.10):

1. Information (i.e. technology), other than software as defined below, material and equipment which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles or included in the U.S. Munitions Lists (USML). Information may be in the form of blueprints, drawings, photographs, plans, instructions, and documentation. Information, material or equipment falling within the above categories also includes that which is still in the “working” or “developmental” stage, regardless of “in

Virginia Polytechnic Institute and State University
Technology Control Plan

process” or “deliverable” status. The release of such information, materials, and equipment via any means (e.g. shipping) or media (e.g. spoken, or written) is not permitted without prime sponsor approval.

2. U.S. Government classified information relating to defense articles and defense services; classified information shall include all documents/information marked by any U.S. federal agency as NOFORN (Not Releasable To Foreign Nationals), Confidential, Secret, and Top Secret.
3. Information covered by an invention secrecy order;
4. Software, as defined below, directly related to defense articles or subject to the Commerce Control List;

Controlled Technical Data does not include information or software concerning general scientific, mathematical or engineering principles currently in the public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. ITAR (22CFR § 120-130) (reference c) NOTE: For security assistance and government contracting purposes, the Security Assistance Management Manual (SAMM para 140104.B) and the Department of Energy Acquisition Regulations ((DEARS) Section 227.401(18)) define “technical data” differently.

Disclosure of unclassified technical data controlled by the International Traffic in Arms Regulations (ITAR) to foreign persons, or unclassified technology or source code controlled by the Export Administration Regulations (EAR) to foreign nationals in the course of employment with U.S. institutions of higher learning is considered an export disclosure. Such disclosure is subject to and requires a U.S. government export license or other government approval prior to disclosure. Administration of the ITAR is conducted by the ODTC Center for Defense Trade, Department of State. Administration of the EAR is conducted by the BIS, Department of Commerce

Individuals must be careful that an unauthorized “release” or transfer action does not inadvertently occur during meetings, telephone conversations, facilities, visits, or other circumstances.

B. Controlled Technology

Controlled Technology (“Technology”) is defined as:

Information, i.e. technology, including scientific information that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment. (DoD Directive 5200.21).

Virginia Polytechnic Institute and State University
Technology Control Plan

“Technology” is also defined under the EAR as specific information necessary for the development, production, or use of a product. The information takes the form of “technical data” or “technical assistance.”

“Technical assistance” may take forms such as instruction, skills training, working knowledge, consulting services.

“Technical data” may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, and read-only memories. (EAR 15 CFR § 772)

There is an important distinction between ITAR-restricted technical data and EAR restricted technology. The threshold for what information constitutes ITAR- restricted technical data is very low- any unclassified information about a defense article that is not information or software concerning general scientific, mathematical or engineering principles currently in the public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. Conversely, the threshold for what constitutes EAR-restricted “technology” is very high, it must be “specific information necessary to develop, produce, or “use” a product listed on the Commerce Control List. Use” is defined as “Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing”

C. Defense Service (22CFR § 120.9.)

A defense service is defined as:

1. “The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles;” or
2. “The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad.”

D. Foreign Persons and Foreign Nationals

ITAR defines a “foreign person” as any person who is not a citizen or national of the U.S. unless that person has been lawfully admitted for permanent residence, (i.e., is under immigrant-visa status, or individuals referred to as “immigrant aliens” under previous laws), in the U.S. under the Immigration and Naturalization Act (8 U.S. C1101, section 101(a) 20, 60 State. 163) and “Protected Individuals” under the INA (8 USC 1324b(a)(3)) designated an asylee or refugee or a temporary resident under amnesty provisions. The definition includes foreign corporations, i.e., corporations that are not incorporated in the U.S.,

Virginia Polytechnic Institute and State University
Technology Control Plan

international organizations, foreign governments and any agency or subdivision of foreign governments (e.g. diplomatic missions).

The EAR defines a “foreign national” as “any person who is not a citizen or national of the United States.” (Note: same as “alien” pursuant to 8 U.S.C. 1101).

The National Industrial Security Program Manual (1995 version) distinguishes between a “foreign national” and an “immigrant alien,” the latter defined as “any person lawfully admitted into the U.S. under an immigration visa for permanent residence” (i.e. one who possesses permanent resident, or immigrant-visa status).

Foreign students that are in the United States on non-permanent resident status are therefore considered foreign persons or foreign nationals.

E. Export and Deemed Export

ITAR (22CFR § 120.17) (reference c) defines “export” as:

1. Sending or taking a defense article out of the U.S. in any manner, except by mere travel outside the U.S. by a person whose personal knowledge includes technical data; or
2. Transferring registration or control to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the U.S. or abroad; or
3. Disclosing (including oral or visual disclosure) or transferring in the U.S. any defense article to an embassy, any agency or subdivision of a foreign government (e.g. diplomatic mission); or
4. Disclosing (including oral or visual disclosure) or transferring controlled technical data to a foreign person, whether in the U.S. or abroad; or
5. Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the U.S. or abroad.

ITAR does not expressly define “deemed export”, however, ITAR 22 CFR § 120.17(4) & (5) are roughly analogous to EAR definitions of “deemed export”.

EAR (15 CFR § 734.2(b)) (reference e) defines “export” as:

1. Sending or taking an article out of the U.S. except by mere personal knowledge, or transferring registration, control, or ownership in the U.S.;

Virginia Polytechnic Institute and State University
Technology Control Plan

2. Disclosing (including oral or visual disclosure) controlled information to a Non-U.S. Person, in the U.S. or abroad;
3. Performing technical assistance, training, or other defense services for, or on behalf of a Non-U.S. Person, whether in the United States or abroad; and
4. Re-exporting from foreign countries items or technology of U.S. origin (including some foreign-made items that incorporate U.S.-origin components or technology).

EAR defines “deemed export” as: “any release of technology or source code subject to the EAR to a foreign national. Such release shall be deemed to be an export to the home country or countries of the foreign national.” (15 CFR § 734.2(b)(ii)). Technology or software is “released” for export through:

1. Visual inspection by foreign nationals of U.S.-origin equipment and facilities;
2. Oral exchanges of information in the United States or abroad; or
3. The application to situations abroad of personal knowledge or technical experience acquired in the United States.

In summary, an ITAR “deemed export” occurs whenever controlled technical data, or source code is released, or defense services is provided, in the U.S or abroad to a foreign person. If an export of technology or source code occurs within the U.S., that action is termed an EAR “deemed” export to the foreign national or foreign person’s country of origin.

F. Equipment and Defense Articles

In general, export of materials, items, or software occur only when they are physically exported outside of the United States, or transferred to a foreign national or foreign person in the United States for the purpose of subsequent export outside of the United States. Access to a material, item, or software in the United States, accompanied by attendant technology or technical data may be considered a deemed export, even in fundamental research.

In proprietary research, access to an export controlled item (including software), material, or defense article, when it includes its access to technology or technical data, or is provided with training on the defense article (a defense service) is a deemed export.

However, in fundamental research, there are significant differences in the two technology-based export control regulations (ITAR/EAR) governing access to export controlled items, materials, or defense articles and their associated technology or technical data. Under ITAR, access to a defense article and its associated technical data, or when a defense service is performed, is an export and is subject to ITAR regulation. Even if the university can meet all

Virginia Polytechnic Institute and State University
Technology Control Plan

other criteria for conducting its research as fundamental, such access to the defense article and its associated technical data is subject to ITAR regulation. The portion of the research involving access to the defense article and its associated technical data must be dealt with as ITAR-restricted technical data.

Under the EAR, equipment with criteria of items listed on the Commerce Control List (CCL) and some of its "use" technology may be used in fundamental research, not subject to export controls unless the item is furnished with technology enabling the foreign national to "develop, produce, or "use" the equipment, "use" as defined in 15 CFR §772.1: "Operation, installation (including on-site installation) maintenance (checking), repair, overhaul, *and* refurbishing." Access to technology that enables the foreign national to perform only a few of these functions is not "use" and is not subject to export control regulation in fundamental research, but access to technology that enables the foreign national to perform all of the functions is a deemed export subject to export control regulation.

G. Software (15 CFR §772.1, 22 CFR §120.10)

Software includes, but is not limited to, the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis, and repair. Under ITAR software is classified as technical data and under EAR software is a category of export controlled items regulated separately from technology.

H. Published Information and Information in the Public Domain (15 CFR § 734.7 and 22 CFR § 120.11)

All information that is currently published, generally accessible, or available to the public. For example:

1. Through sales at news stands and bookstores;
2. Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; or
3. At libraries open to the public or from which the public can obtain documents;
4. Through issued patents;
5. Fundamental Research: ITAR: (22 CFR § 120.11(8)) Basic and applied research in science and engineering at accredited institutions of higher learning, in the United States, in which the resulting information can be published and shared broadly within the scientific community. Such research is termed "fundamental research" and is not subject to security classification or export control procedures. However, sponsored research conducted by a university is not considered "fundamental research" if:
 - i. The University or its researchers accept sponsor's restrictions on publication of scientific and technical information resulting from the project ; or,

Virginia Polytechnic Institute and State University
Technology Control Plan

- ii. The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable
6. Fundamental Research: EAR: (15 CFR § 734.8) Research conducted by scientists, engineers, or students at a university normally will be considered fundamental research. (“University” means any accredited institution of higher education located in the United States.) Prepublication review by a sponsor of university research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers does not change the status of the research as fundamental research. However, release of information from a corporate sponsor to university researchers where the research results are subject to prepublication review is subject to the EAR. Prepublication review by a sponsor of university research solely to ensure that publication would not compromise patent rights does not change the status of fundamental research, so long as the review causes no more than a temporary delay in publication of the research results.

If research is funded by the U.S. Government (15 CFR § 734.11), and specific national security controls are agreed on to protect information resulting from the research, 15 CFR §734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific controls may nonetheless be made under this provision.

Fundamental research is not subject to export control regulation, and there are no restrictions on participation in fundamental research by foreign nationals. Procedures for conducting Sponsored Projects that are subject to export controls are established in OSP 29-05 Management of Export Controlled Sponsored Projects.

There is an important distinction between the ITAR-defined fundamental research, and the EAR-defined fundamental research. ITAR-defined fundamental research is void when the research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable. Under the EAR, access restrictions alone void the university’s fundamental research exclusion. Thus, in government funded research, it is possible to have foreign national access restrictions if there are no dissemination controls on the research, and the results may be disseminated widely. No such fundamental research is possible under the EAR.

- I. U.S. Government Classified Technical Data, Material, Items (e.g., contracts that incorporate Federal Acquisition Regulations (FAR) Clause “Security Requirements,” 52.204-2, or DEARS 952.204-2).

Virginia Polytechnic Institute and State University
Technology Control Plan

Classified Information is releasable only to those individuals (e.g. employees, graduate students, visitors, etc.) with the appropriate U.S. security clearance (confidential, secret, top secret, etc.) and the appropriate need-to-know, as determined by the possessor of the classified information. The handling of classified information is discussed in detail with the Principal Investigator and the University's Facility Security Officer. Classified information is not authorized for release or disclosure to any foreign national. No classified access will be provided to the foreign national, thereby prohibiting access to facilities, documentation, and records, as well as prohibiting foreign nationals access to design, development, and test areas where classified work is in process.

Foreign nationals will not be authorized access to classified contracts without proper authority.

1. Unclassified Controlled Technical Data

a.

Foreign persons/foreign nationals can not be granted access to controlled technical data or technology without appropriate export license or other government approval (i.e., a license exemption or license exception) from ODTC or BIS as appropriate. Prior to acceptance of a sponsored project with export control restrictions, the Principal Investigator and Office of Export and Secure Research Compliance (ESRC) shall prepare a project specific TCP prior to their participation in the project, unless this requirement is waived by the ESRC Director.

b.

If the publication or any disclosure of the project's findings is subject to approval by the contracting officer, once that approval is received, the information contained in that disclosure can therefore be placed in the "public domain" and, consequently, is no longer considered export controlled.

2. Proprietary Information

- a. Virginia Tech Proprietary Information is protected internally by confidential invention disclosures and internal nondisclosure agreements as may be necessary. Release of Virginia Tech proprietary information externally occurs only after a nondisclosure agreement is executed between the party receiving the information.
- b. Proprietary Information received by Virginia Tech is protected under the terms of each individual nondisclosure agreement as may be negotiated and executed by the parties involved unless the information is required to be released by a court of competent jurisdiction or as otherwise required under legal proceedings.

Proprietary information is subject to ITAR and EAR export regulations.

VI. Education

Academic departments will be responsible for appropriate orientation of all new employees, graduate, and undergraduate students, including foreign nationals employed by their departments for projects that fall within this Technology Control Plan. When appropriate, foreign nationals will be briefed and/or informed concerning those areas of export control and export licensing actions that are pertinent to their activities. ESRC will make available export awareness training to university personnel.

VII. Export Controlled Research and International Collaborations

Acceptance of an export control restricted research project or international collaboration places Virginia Tech at risk of inadvertent violation of export laws. Principal Investigators shall coordinate with ESRC to determine if a proposed research project or international collaboration is subject to export restrictions. The ESRC will assist each Principal Investigator in determining the appropriate export regime and if subject to export regulation, the project-specific security measures needed to prevent unauthorized export of restricted defense articles, items, technical data, technology, and software. Principal Investigators for any identified export controlled projects shall submit to the ESRC a Project-specific Technology Control Plan prior to the initiation of the project.

In addition to ITAR and EAR export restrictions, OFAC regulates the following transactions with sanctioned countries, entities, and individuals (31 CFR § 500)

- i. Transactions involving designated foreign countries or their nationals;
- ii. Transactions with respect to securities registered or inscribed in the name of a designated national;
- iii. Importation of and dealings in certain merchandise; and
- iv. Holding certain types of blocked property in interest-bearing accounts.
- v. Transactions with specific entities or individuals known as “specially designated nationals,” found in the Specially Designated Nationals List ("SDNL"),

In many cases a license from OFAC is required in order to travel to, or have transactions with sanctioned countries. University personnel will not engage in international collaborations with sanctioned countries, entities, or individuals without first consulting with ESRC to determine if an OFAC license is required.

Principal Investigators for any international collaboration that meets the criteria of fundamental research, or does not involve technology transfer shall sign a faculty agreement (Attachment E) acknowledging his/her responsibilities to comply with export regulations in the international collaboration, as will all Virginia Tech participants in the international collaboration.

Virginia Polytechnic Institute and State University
Technology Control Plan

VIII. Administration

Administration of this TCP is the responsibility of the University's Technical Control Plan Officer, who is also the Export Control Program Manager (ECPM), assigned to the Office of Research Compliance, as it applies to the release of controlled technical data of U.S. origin in a foreign country or to a foreign person/national or entity. The ECPM will request a counterintelligence briefing visit from the Defense Security Service on an annual basis.

Principal Investigators and/or department heads are responsible for ensuring that employees in their activities are properly instructed in the handling of classified, , export-controlled, or sensitive information and that they have signed or submitted the required briefing document:

1. Technology Control Plan Briefing (Attachment A) *Applicable to Classified Projects.*
2. Foreign National's Nondisclosure Statement (Attachment B) *Applicable to Foreign Nationals/Foreign Persons with a license for access to export controlled commodities, software, or technical data.*
3. Bona Fide Employee Letter (Attachment C) *Applicable to Virginia Tech employees who are exempt from ITAR export control restrictions as a Bona Fide Employee of the University.*
4. Project Specific Technology Control Plan (Attachment D) Example Only *Applicable when the University accepts an export controlled or similarly restricted Sponsored Project.*
5. Faculty/Participant Agreement for use with International Agreements (Attachment E) Example Only. *Applicable when the University accepts an international collaboration with export control risk.*

The Technology Control Plan Officer (TCPO) shall prepare and maintain the University's Technology Control Plan.

The TCPO shall prepare and maintain Office of Sponsored Programs policy OSP-29-05 "Management of Export Controlled Sponsored Projects," Other University management personnel supporting the TCPO's implementation and administration include:

Vice President for Research
Director, Office of Export and Secure Research Compliance
Special Assistant Research Contract Affairs, VP for Research Office
Assistant Vice President for Administration, Sponsored Programs

IX. Freedom of Information

As a public educational institution of the State of Virginia, Virginia Tech has certain obligations to respond to requests for "public" information. However, not all information of the University is subject to state statutes and each request for information is reviewed by appropriate

Virginia Polytechnic Institute and State University
Technology Control Plan

administrators/University Counsel for our legal obligations for release or protection of the information. Virginia Tech believes sufficient control and supervision will exist in regard to all employees, undergraduate and graduate students, including those with foreign national status, as regards technology transfer or release of technical know-how. It is the intention of Virginia Tech to protect all its information not in the public domain unless appropriately authorized by a court of competent jurisdiction, applicable state statute, or the U.S. Government as may be required in each individual case.

In order for Virginia Tech to assume responsibility to meet federal regulations previously cited, no employee, graduate/undergraduate student or other person acting on behalf of Virginia Tech shall disclose or release controlled technical data, technology or source code, as herein defined, without full compliance to this policy document.

Virginia Polytechnic Institute and State University
Technology Control Plan

ATTACHMENT A

TECHNOLOGY CONTROL PLAN BRIEFING
Applicable to Classified Projects

Project Account:

Sponsor Name & Project Title:

This is to acknowledge that I, _____, have read the Virginia Tech University Technology Control Plan and have discussed the plan with the Virginia Tech Facility Security Officer, or his designee, and that I understand the plan and agree to comply with its requirements.

(Signature) Date

(Printed Name)

Acknowledgement of Immediate Supervisor:

(Signature) Date

(Printed Name)

ATTACHMENT B

Foreign National's Nondisclosure Statement*

*Applicable to Foreign Nationals/Foreign Persons with a license
for access to export controlled commodities, software, or technical data/technology*

Project Account:

Sponsor Name & Project Title:

I, _____, as a Foreign National, acknowledge and understand that any technical data related to defense articles on the U.S. Munitions List, to which I have access or which is disclosed to me in the course of my association with Virginia Tech, is subject to export control under international Traffic in Arms Regulations (Title 22, Code of Federal Regulations, Parts 120-130) and/or Export Administration Act (Pub. L. 96-72), (50- USC 2401-2420). I hereby certify that such data will not be further disclosed, exported, or transferred in any manner to any other foreign national or any foreign country without approval from the Office of Munitions Control, U.S. Department of State.

(Signature) Date

(Printed Name)

Acknowledgement of Immediate Supervisor:

(Signature) Date

(Printed Name)

*This statement is to be completed only after a license to export to the named individual has been received from the U.S. Department of State or Commerce, as applicable.

Bona Fide Employee Letter

Applicable to Virginia Tech employees who are exempt from ITAR export control restrictions as a Bona Fide Employee of the University

VIRGINIA POLYTECHNIC INSTITUTE
AND STATE UNIVERSITY

Office of Export and Secure Research Compliance

2000 Kraft Drive, Suite 2000
Blacksburg, Virginia 24060
Phone (540) 231-3801 Fax: (540) 231-0959

Dear :

You are hereby notified that as _____ (*participant/principal investigator*) in the Sponsored Project for

_____ (*name of project*) you will be producing International Traffic in Arms (ITAR) export control restricted experimental or developmental electronic equipment specifically designed or modified for military application or specifically designed or modified for use with a military system and associated technical data.

In accordance with ITAR 22 CFR § 125.4(b)(10), the ITAR-restricted defense articles or technical data may not be transferred to foreign persons without the prior written approval of the Office of Defense Trade Controls. Prohibited technical transfer includes oral, visual, written or electronic disclosure, as well as transfer of physical custody. Violations of International Traffic in Arms Regulations can result in criminal penalties of up to 10 years in prison and \$1 Million in fines, and civil penalties of up to \$500,000 in fines and forfeiture (22 CFR §§ 127-1 through 127-12).

If you have questions about this export control restriction, please contact David Brady (540-231-3801) from our office.

Sincerely,

David A. Brady
Director, Office of Export and Secure Research
Compliance

University File

Foreign Person Technology Control Plan
for Virginia Polytechnic Institute and State University
for the [Insert Project Name]
for the [Insert Government or flow through and Government sponsor]

Institutional Commitment

Virginia Polytechnic Institute and State University (“Virginia Tech”) is committed to complying with applicable export control laws. To ensure compliance with these laws in sponsored programs, this project will be managed in accordance with OSP Policy 29-05 Management of Export Controlled Sponsored Projects.

Commodity Jurisdiction and Classification *[PI and Director, Export and Secure Research Compliance will prepare this section]* There are *[insert applicable restriction or reason the project is subject to ITAR restrictions]* restrictions on this research project. Based on the determination of the sponsor, this project is ITAR-restricted under *[specify ITAR Category from 22CFR 120.1]* and includes:*[Specify category subheadings that are applicable]*

The Project will *[specify project objectives]*

The technical data generated in this project and micromechanical model developed from this data are restricted as technical data under ITAR Category IV (i). Project deliverables, and supporting documentation and data are restricted under ITAR Category IV(i). No Category IV defense articles will be developed or produced in this project. s.

As a result of this determination, the Principal Investigator, *[Insert PI name]* has adopted a foreign person technology control plan to ensure that controlled defense articles, software, and technical data are adequately protected from disclosure to foreign persons who do not have an approved license or valid license exception from the government. The plan addresses physical security, information security, personnel screening procedures and training. These plans are described in detail below.

Physical Security Measures *[PI edit as applicable to meet specific project/lab conditions]*

Computing machineries used for this project include faculty workstations that reside in their offices, and a mobile workstation used by the graduate research assistant in the XXXXXXXX Lab (XXXXXXXXXXXXXXXXXX). Students do not have physical access to the faculty workstations. Some of the faculty workstations are laptops that are also used at the faculty’s private residences. The project investigators are the sole designated users of their workstations at either their home or office. Faculty and cleaning / maintenance / security staff are the only authorized key holders to the offices. Faculty offices and the XXXXXXXXX Lab are located in segregated sections of XXXXXXXX Hall. Access to the XXXXXXXXXX Lab requires a personalized keycard at all times.

Information Security Measures *[PI edit as applicable to meet specific project/lab conditions]*

All workstations run OS X or Microsoft Windows XP with the latest security service pack and patches. The faculty are required to provide a valid account and password to gain access to their machine. Only the investigators retain login information (username and password) to their workstations. The login information is not shared with anyone nor are other login accounts created for access to the workstation. The account restriction also applies to the graduate research assistant’s workstation. Both failed and successful logins are logged internally. User files that contain sensitive data provided by the sponsor for this project are stored in an encrypted storage medium. Files transfers related to this project are made only between the faculty and the graduate research assistant. Firewalls are installed on each of the machines to secure and monitor network access from/to the machines. Backups are maintained by the respective user of each machine and will be kept within the faculty offices. Hard copies that contain information provided directly by the sponsor or information derived from sponsor data will be stored in the PI’s office. Otherwise, hard copies will be immediately and securely disposed.

Code, data or documents provided by the sponsor, or derived from the sponsor’s code, data or documents will be stored in a locked room (XXXXXX) reserved for this purpose. Access is restricted to project personnel and

maintenance / security staff. A log will be maintained of files or documents checked out for meetings or work sessions. All backup media will permanently reside in XXXXXXXXXXXXXXXX.

Printed copies of files that contain information provided directly by the sponsor or information derived by sponsor data will be marked with the warning:

This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.). Violations of these export laws are subject to severe criminal penalties.

Tracking and secure disposal procedures will be used for these hardcopies. . Emails shall not contain ITAR-restricted technical data or files unless both send and receive email locations are encrypted.

Personnel Screening Procedures

All project personnel have attended or will attend export control training provided by the University’s Office of Export and Secure Research Compliance (ESRC). Personnel who have not had training before having access to export controlled commodities, technology, or software will review this Plan and sign Attachment A. All project personnel are made aware of their responsibilities to prevent either active or inadvertent disclosure of ITAR-restricted defense articles, software, and technical data, and of the criminal and civil penalties (including prison sentences of up to 10 years and fines of up to \$1M) for failure to comply with U.S. export control rules. Non-project personnel are also informed of their obligations, and the consequences for possessing or disseminating ITAR-restricted information. All Project personnel have been screened by ESRC against the applicable restricted parties’ access lists.

Self Assessment

The PI and department shall notify OSP (1) each time an additional person is added to the project so that they can be screened and trained, and (2) when the scope of the project changes. The PI will annually certify, by 31 December, and the (*department/ center/college*) shall approve that the project is being carried out in compliance with this TCP.

Submitted:

PI: (*Print name*)

(*Department/College/ Center*)

By: _____

By: _____

Name:

Name:

Title: Principal Investigator

____Title: (*Director /Department Head/Dean*)

Date: _____

Date: _____

**Attachment E: Acknowledgement of Technology Control Plan
for Virginia Polytechnic Institute and State University
for the [Insert Project Name]
for the [Insert Government or flow through and Government sponsor]**

I hereby certify that I have read and understand the provisions of the above Technology Control Plan, as well as understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export controlled information to unauthorized persons.

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

ATTACHMENT F: FACULTY AGREEMENT

FOR USE WITH INTERNATIONAL AGREEMENTS-

Insert Program Name Here

This form is for internal use only and should not be forwarded to the sponsor or collaborator.

The Office of Sponsored Programs (OSP) has negotiated on your behalf an international agreement which may involve the transfer of export controlled equipment, materials, software and/ or the release of export controlled information to a foreign country or foreign nationals which may require a license or other government approval.

Export Controlled Equipment, Software, Technology, and Transactions

Yes No Please read each statement carefully and acknowledge yes or no.

 Release of Nonpublic Information and Software. I understand that the U. S. government restricts the export of certain items and technology and that Virginia Tech and all its employees must comply with these laws. In the international project, I shall only release published information or software, educational information, and information resulting from fundamental research (see definitions on the following page) without confirming with the Office of Export and Secure Research Compliance (ESRC) whether or not a government export license or other government approval is required, and if such is required, a license or other government approval is obtained.

 Export of Equipment/Items. I understand that it may be unlawful to export equipment, software, materials, and other items subject to export regulations without a license or other government approval. I will consult with the ESRC before shipping, sending, or taking overseas any equipment, software, materials, or other items related to the international project.

 Defense Articles. I understand that most military and some civilian equipment, software, and their associated technical data are restricted for export, and providing foreign nationals any access to, training on, or technical data related to these items to may require an export license or other government approval. International Traffic in Arms Regulations (ITAR)-restricted civilian items include but are not limited to spacecraft systems and associated equipment (including satellites), Y-Code GPS; some aircraft and associated equipment, including Inertial Measurement Units (IMUs), developmental aircraft, engines, and components, and unmanned aerial vehicles (UAVs). Before disclosing information relating to military or other defense articles to any foreign national, I will consult with ESRC.

 Sanctioned Countries, Entities, and Persons. I understand that Virginia Tech and its employees are prohibited by law from doing business with some countries sanctioned by the United States Government, and with persons and entities on the Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons List (SDN). Before traveling overseas in the international project, I will obtain an update on sanctioned countries and on the SDN from ESRC.

CONCURRENCE

I will ensure that all Virginia Tech participants in this International Agreement will sign a Participant Agreement. I understand that failure to abide by these terms and conditions may result in an unlawful export of controlled items, software, or technology, or an unlawful transaction with a sanctioned country, entity, or person for which I may be personally liable for civil and criminal punishment including fines and imprisonment.

Principal Investigator	Date	Investigator	Date
Investigator	Date	Investigator	Date

DEFINITIONS

Published Information and Software: Information is generally accessible to the interested public in any form, including:

(1) Publication in periodicals, books, print, electronic, or any other media available for general distribution to any member of the public or to a community of persons interested in the subject matter, such as those in a scientific or engineering discipline, either free or at a price that does not exceed the cost of reproduction and distribution ;

(2) Ready availability at libraries open to the public or at university libraries

(3) Patents and open (published) patent applications available at any patent office; and

(4) Release at an open conference, meeting, seminar, trade show, or other open gathering.

(i) A conference or gathering is “open” if all technically qualified members of the public are eligible to attend and attendees are permitted to take notes or otherwise make a personal record (not necessarily a recording) of the proceedings and presentations.

(ii) All technically qualified members of the public may be considered eligible to attend a conference or other gathering notwithstanding a registration fee reasonably related to cost and reflecting an intention that all interested and technically qualified persons be able to attend, or a limitation on actual attendance, as long as attendees either are the first who have applied or are selected on the basis of relevant scientific or technical competence, experience, or responsibility

(iii) “Publication” includes submission of papers to domestic or foreign editors or reviewers of journals, or to organizers of open conferences or other open gatherings, with the understanding that the papers will be made publicly available if favorably received

Software and information is published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution.

Notwithstanding paragraphs (a) and (b) of this section, note that some encryption software controlled and mass market encryption software with symmetric key length exceeding 64-bits may be subject to export regulations.

Educational Information: “Educational information” is not subject to the Export Administration Regulations (EAR) if it is released by instruction in catalog courses and associated teaching laboratories of academic institutions. Note that the provisions of this section do not apply to some encryption software or to mass market encryption software with symmetric key length exceeding 64-bits for certain exports and reexports under license exception.

Fundamental Research: University-based basic or applied research conducted by scientists, engineers, or students at any accredited United States institution of higher education. University based research is not considered “fundamental research” if the university or its researchers accept (at the request, for example, of an industrial sponsor) other restrictions on publication of scientific and technical information resulting from the project or activity; including foreign national access and dissemination controls. Scientific and technical information resulting from the research will nonetheless qualify as fundamental research once all such restrictions have expired or have been removed.

Foreign National: A person or entity that is not a U.S. Person.

U.S. Person is (1) a U.S. citizen, (2) an alien who are “Lawful Permanent Residents” (Green Card holder) (8 USC § 1101(a)(20)), (3) “Protected Individuals” under the INA (8 USC §1324b(a)(3)) designated an asylee or refugee, or a temporary resident under amnesty provisions; and (4) any entity incorporated to do business in the U.S.