



SAINT LOUIS UNIVERSITY

Export Control Policy

Policy Number: OUC-021

Version Number: 1.0

Effective Date: May 11, 2016

Responsible University Official: Vice President and General Counsel

Approved By: Executive Staff (05/11/2016)

1.0 INTRODUCTION

Saint Louis University strives to be fully compliant with federal export control regulations while maintaining an open and collaborative academic environment. For reasons of national security and/or protection of trade, certain activities within the University are subject to U.S. export control laws and regulations.

Federal export control laws and regulations apply to all activities undertaken by Saint Louis University faculty, staff, students, and other persons at the University acting on behalf of the University that involve the following:

1. Shipping tangible items outside the United States;
2. Sharing proprietary, confidential, or restricted information or software code with foreign nationals within the United States or abroad;
3. Interactions with embargoed or sanctioned countries, organizations, or individuals (Restricted Parties) (including purchases from foreign suppliers);
4. Travel to a foreign country with controlled technologies/information including laptops, mobile phones, and portable storage devices.

2.0 PURPOSE

The purpose of this policy is to ensure the University maintains compliance with Federal Export Control laws and regulations including: Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), and the Office of Foreign Assets Control (OFAC). This policy outlines procedures designed to implement reasonable and appropriate safeguards to prevent unauthorized access to controlled information, while allowing authorized personnel access to information necessary to complete their work.

3.0 PERSONNEL AFFECTED

This policy applies to all Saint Louis University faculty, staff, students, and those associated with the University on a temporary basis such as visitors and visiting scholars.

4.0 DEFINITIONS

Deemed Export- Providing access in any manner or discussing controlled research with foreign nationals on U.S. soil.

Defense Article- Any item or technical data designated on the United States Munitions List. (ITAR § 121.1)

Dual-Use- Items or technologies that have both commercial and military or proliferation applications.

EAR- Department of Commerce, Export Administration Regulations 15 CFR 730-774. Regulates “Dual-use” items; commercial goods, services, and technologies that also have military or proliferation possibility. (i.e. Phased Array Antennae)

Empowered Official- The appointed individual at the University legally authorized to sign export license applications and other authorizations required by export control laws and regulations on behalf of the University. The Vice President and General Counsel is the University’s Empowered Official for all purposes relating to the applicable federal export control laws and regulations as defined in 22 CFR 120.25.

Export- Any item, technology, or software sent from the United States to a foreign destination; these Exports are not limited to tangible items. Any email, in-person or phone conversation, letter, or travel to a foreign national or foreign destination is considered an Export.

Export Control Officer- The University employee charged with compliance of federal export control regulations.

Foreign National- Any individual that is not a U.S. person; “Foreign Nationals” can also include any business, organizations, or entities that are not licensed to do business within the borders of the United States.

Fundamental Research- Basic and applied research in science and engineering where the resulting information is to be shared broadly within the scientific community.

ITAR- Department of State: International Traffic in Arms Regulations 22 CFR 120-130. Regulates defense items; products specifically designed for military applications.

OFAC- Department of the Treasury, Office of Foreign Assets Control 31 CFR 500-599. Regulations pertain to countries, organizations, and individuals; Financial focus; targets-terrorists, drug traffickers, weapons of mass destruction proliferators, narcotics, human rights violators.

Restricted Parties- Individuals and entities with whom the University and its employees may be prohibited by law, or that require a license or other government approval, to export to or engage in controlled transactions. These include individuals and entities listed on the Denied Persons List, Entity List, and Unverified List (Department of Commerce); the Debarred Parties List (Department of State); and the Specially Designated Nationals and Blocked Persons List (Department of Treasury).

Technology Control Plan- A written plan created by the Export Control Officer, with assistance from the Principal Investigator (PI), stipulating how the controlled aspects of the research will be secured.

Temporary Export Certificate- Document used to identify University equipment that will be exported only temporarily with intent to return to United States.

Use- Operation, installation (including on-site installation), maintenance (checking), repair, overhaul, or refurbishing.

U.S. Person- Any person who is a citizen of the United States, a lawful permanent resident alien of the United States, a refugee or someone in the United States under amnesty.

5.0 POLICY

No person affiliated with Saint Louis University may export items or make deemed exports contrary to the requirements of the federal export laws, regulations, or any policies and procedures of the University. Research at Saint Louis University must be conducted in full compliance with all applicable federal export control laws and regulations, as well as University policies and procedures.

5.1 Guiding regulations

5.1.1 Export Controls are primarily regulated by three federal agencies:

1. Commerce Department **Export Administration Regulations**
15 CFR 730-774

The Commerce Department's Bureau of Industry and Security (BIS) implements and enforces U.S. export control regulations relating to the export of civil and dual-use goods and technologies, which have both civil and military applications. Items subject to the jurisdiction of BIS are listed on the Commerce Control List. BIS also maintains the Denied Persons List and

Denied Entities List that identify specific persons and entities to which exports are not permitted without the prior approval of BIS.

2. State Department **International Traffic in Arms Regulations**
22 CFR 120-130

The Directorate of Defense Trade Controls (DDTC) of the U.S. Department of State is responsible for items and information that have military applications (via their design, purpose, or use). Tangible items are referred to as “defense articles.” Information related to defense articles is referred to as “technical data.” Controlled defense articles and space related items can be found on the U.S. Munitions List (22 CFR 121).

3. Treasury Department **Office of Foreign Assets Control Targeted Economic Sanctions Program**
31 CFR 500-599

The U.S. Treasury Department oversees economic sanctions and embargoes through the Office of Foreign Assets Control (OFAC). OFAC has broad authority to enforce export controls under the Trading with the Enemy Act (12 USC 95) and the International Emergency Economic Powers Act (50 USC 1701). OFAC has the ability to block or interdict “prohibited transactions” involving restricted destinations or parties.

5.1.2 Exclusions and Exemptions

1. **Fundamental Research Exclusion (FRE)**

Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

The FRE only applies to the dissemination of research data and information, not to the transmission of goods. The FRE does not apply to a sponsor’s existing proprietary information when some or all of that information is required to be held confidential. The FRE will not apply to physical goods, software, encryption, research where there is no intent to publish, and research conducted outside the United States.

2. **Educational Exclusion**

According to EAR, publicly available "educational information" is not subject to the EAR if it is released by instruction in catalogue courses and associated

teaching laboratories of academic institutions (see 15 CFR 734.3(b)(3) and 734.9).

Per ITAR, information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities are not subject to ITAR (see 22 CFR 120.10(a)(5)).

3. **Public Information Exclusion**

Information that is published and generally accessible or available to the public is not controlled under the EAR or ITAR. The specifications on what information qualifies as publicly available vary between the EAR (publicly available) and ITAR (public domain).

“Publicly available” according to EAR means printed and published materials, prerecorded phonographic records, exposed or developed microfilm, motion picture film and soundtracks, reproducing printed and published content, or software and technology that have been or will be published; arise from fundamental research; are educational; or are included in certain patent applications (see 15 CFR 734.3(b)(3) and 734.7).

Per ITAR, “Public Domain” means information that is published and generally accessible or available to the public, through sale at newsstands and bookstores, through subscriptions available without restriction, through distribution at a conference open to the public, through any patent office, and through libraries, if accessible by the public; or public release of controlled technical data “in any form” (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency; or fundamental research (see 22 CFR 120.11).

4. **Bona Fide Full-Time Employees**

ITAR (§125.4(b)(10)) provides an exemption allowing universities to disclose unclassified technical data in the United States to a foreign person who is a University’s bona fide full-time regular employee if all of the following are true:

- The employee's permanent abode throughout the period of employment is in the United States;
- The employee is not a national of a country to which exports are prohibited pursuant to ITAR § 126.1 (embargoed countries);
- The University informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of the DDTC.

The application of this exemption is more limited than the FRE and public domain exemptions. Graduate students and post-docs may not be considered to be regular full-time University employees, and disclosures to them would not qualify for this exemption.

5.2 Sharing of Information

Sharing regulated information or research with Foreign Nationals who do not have a federal license to view information or research is prohibited.

U.S. citizens providing training or technical assistance to foreign nationals where controlled technology is involved requires an export license.

5.3 Accepting a Third Party's Controlled Items or Data

Fundamental research projects may require third-party equipment or technology that is subject to export control restrictions. Proprietary or restricted information that is required for the development, production, or use of export controlled equipment is itself export controlled. The export control requirements for such third party items or data must be honored by the researcher who agrees to receive such information. In such cases the Principal Investigator (PI) must contact the Export Control Officer to obtain an export control determination and develop a Technology Control Plan (see 5.8 below) before accepting the controlled items or data. The primary determinate of acceptability of such projects will be those with no restrictions on publication of significant elements of the research results.

In the event an individual at the University believes they have been sent controlled items or data for which no special arrangements were previously made, they must immediately attempt to safeguard the information and contact the Export Control Officer. An example of this would be if a PI receives an unexpected email containing information believed to be export controlled.

5.4 Shipping

Export control regulations always apply to the export of tangible items and may require an export license depending on the item, its destination, and the recipient. Principal Investigators must contact the Export Control Officer to obtain certification of the export control determination before tangible items are shipped outside the United States.

Shipments of regulated materials and letters, conversations – either by phone or in person - and emails pertaining to regulated information or research to a foreign destination without federal licenses is strictly prohibited.

5.5 Travel

International travel to meetings, seminars, and other professional events outside the United States may be subject to licensing requirements. Special attention should be given by those traveling with University equipment (i.e. laptops, mobile phones, and portable storage devices). University faculty, staff, and students must ensure that there is no export controlled information contained on such devices unless there is a specific license or other authorization in place for that information for that destination.

It is prohibited for University faculty, staff, and students to travel with regulated information and research to a foreign destination. Travel to countries subject to embargo and/or a sanction is subject to further restrictions or may be prohibited by export control laws and regulations.

Individuals traveling to foreign destinations are responsible for accurately answering the Export Control questions within the centralized University travel system. The traveler may be required to further provide information to the Export Control Officer regarding their trip, data, technology being carried or affiliates they plan to meet, to determine whether approval or licenses are necessary. If necessary, University faculty, staff, and/or students will be briefed on the regulations, requirements, limitations, and provisos governing their overseas activities prior to their traveling outside the United States. The Export Control Officer in conjunction with the faculty/staff/student will request the exemption or license to travel.

Saint Louis University will mirror the federal government's policy of denial for comprehensive sanctioned countries. If a member of the University community places the University at risk for Export Control penalties by traveling to a regulated country without proper authority, the Export Control Officer has authority to suspend travel.

5.6 Research Agreements

5.6.1 Confidentiality Agreements and Nondisclosure Agreements

In order to maintain the FRE, research projects must be free from restrictions on publication and involve information that is not subject to access or dissemination controls. Under the EAR, access and dissemination controls do not include limited prepublication reviews to prevent the disclosure of proprietary information or to preserve patent rights. Other forms of prepublication review could nullify the FRE, which can result in serious consequences such as having to restrict foreign student participation, loss of federal funding, and increased risk for violation of the export control regulations.

Confidential Disclosure Agreement (CDA) is also known as a Confidentiality Agreement and/or a Non-Disclosure Agreement (NDA). The sponsor or third-party will require such agreements before they release confidential, proprietary, or restricted information to a researcher. These CDAs and NDAs are usually negotiated as part of a larger set of institutional agreements between the University and a sponsor or third party. These agreements are reviewed and negotiated by the Office of Research Development and Services and the Office of Sponsored Programs Administration. If an agreement refers to export controls, it will also be reviewed by the Export Control Officer. These offices have signature authority to bind the University in such agreements. An individual researcher cannot sign such agreements on behalf of the University.

5.6.2 Anti-boycott Provisions

Federal law prohibits any U.S. person from participating in any non-U.S. sanctioned foreign boycott (EAR §760). The primary example is the Arab League boycott of Israel. Examples of participation include:

- Agreements to refuse, or actual refusal, to do business with or in Israel or with blacklisted companies,
- Agreements to discriminate, or actual discrimination, against other persons based on race, religion, sex, national origin, or nationality,
- Agreements to furnish, or actual furnishing, of information about business relationships with or in Israel or with blacklisted companies; or
- Agreements to furnish, or actual furnishing, of information about the race, religion, sex, or national origin of another person.

The University is required to promptly report any occurrences of restrictive trade practices to the government (see also 26 USC 999; 26 CFR 7.999). University faculty, staff, or students who receive a request to participate in any boycott must immediately notify the Export Control Officer or the Office of Sponsored Programs Administration.

5.7 Administration

The Vice President and General Counsel is the Empowered Official at Saint Louis University responsible for the execution of licenses and for the ultimate management and control of this policy. The Export Control Officer, under the direction of the Executive Director of Compliance is responsible for the oversight and administration of this policy. Additional support and services related to export controls at the University are provided by the Information Technology Services, Division of Business and Finance, Human Resources, Office of International Services, and Research Administration.

5.8 Technology Control Plans

All University departments that possess export controlled items (i.e., equipment, software, or technical data) are responsible for providing and maintaining the appropriate security of controlled items and related documentation. Before a department obtains controlled items, a Technology Control Plan (TCP) must be in place.

The purpose of a TCP is to protect technical information which is not covered under exemption by the export control laws and regulations. A TCP provides guidelines to ensure that the information is not transferred to a foreign person or persons unless approved by license with the Department of State, Office of Defense Controls (ODTC), or Department of Commerce, as applicable.

All authorized personnel listed on the TCP must receive restricted party screening by the Export Control Officer. The finalized TCP shall be reviewed and approved by the Export Control Officer. The PI must review the TCP with all project personnel before they begin work on the project, and the TCP must be signed by the PI and other relevant personnel. Training in export controls is required of all personnel involved in projects with a TCP. Periodic audits of the TCP will be conducted. The TCP must be amended, by the PI, when a new member of the research team has been approved, or if the scope of work changes. The PI must notify the Export Control Officer of any changes.

If a contract or other agreement contains language restricting the publication of research results beyond 90 days, and/or for reasons other than the review of patent or proprietary sponsor information, a TCP may also be required. If applicable, the TCP must include a signed certification by the PI and participating graduate student(s) acknowledging that the publication restrictions on that project may adversely affect their ability to complete a thesis/dissertation involving any export controls items or data.

5.9 Documentation Retention

Principal Investigators must keep electronic or hard copies of all export documentation including financial records and shipping documentation (FedEX forms, commercial invoices, purchase orders, etc.) and University export certification documents in their project files for a period of five years from the date of export, re-export, or transfer of a tangible item abroad or of controlled information to a foreign national either outside or within the United States (see EAR §762.6; ITAR §130.14). All documents must be kept in a locked file cabinet, locked or access-controlled office or laboratory, or other secured location. Records must be kept in a manner that facilitates retrieval for review during internal or U.S. government audits.

5.10 Internal Reviews

Periodic reviews of Technology Control Plans and Export Control procedures will be conducted by the Export Control Officer and the University Compliance Office.

5.11 Training Requirements

Researchers must complete export controls training before beginning work on any EAR or ITAR controlled project.

6.0 RESPONSIBILITIES

6.1 Export Control Officer shall:

1. Establish, maintain and publish policies and procedures to ensure compliance with Export Control laws and regulations;
2. Review foreign travel of faculty, staff and students to verify compliance with Export Control regulations and laws;
3. Monitor research proposal submissions in order to screen projects, people, and entities for activities involving embargoed or sanctioned countries, organizations, and/or individuals;
4. Prepare technology control plans;
5. Provide staffing to serve as liaison with University employees concerning export controls;
6. Design and implement an Export Controls Training Program for faculty, staff, and students at the University. Recommend or require training for specific situations involving export controls;
7. Document and maintain export control training in accordance with any applicable federal guidelines on record keeping; and
8. Notify the appropriate federal agencies of export control violations in a timely manner.

6.2 Office of University Compliance shall:

1. Periodically review the Technology Control Plans and procedures to verify that the investigators, Export Control Officer, Human Resources, ITS, Research Administration and International Center are properly following the federal export control regulations and this policy;
2. Notify the Export Control Officer and coordinate the investigation of concerns conveyed through the Compliance Hotline or other means regarding suspected violations of export control regulations and University policy.

6.3 Information Technology Services shall:

1. Provide a point of contact for notification of export control issues regarding technology (e.g., data, computers, cell phones, laptops, portable storage devices);
2. Appropriately staff roles required to support users and locations impacted by export controls;
3. Develop and maintain standard operating procedures for delivery of information technology service in export control designated labs;
4. Educate information technology staff on the importance and relevance of export controls;
5. Participate in review of Technology Control Plans in conjunction with the Export Control Officer; and
6. Assist faculty and staff in identifying technical options and mechanisms for achieving compliance with export controls.

6.4 Office of International Services shall:

1. Facilitate access for the Export Control Officer to reports listing all international students at Saint Louis University at least once every fall and spring semester;
2. Provide names of visiting faculty to Export Control Officer for Restricted Party Screening as needed;
3. Provide names to Export Control Officer of potential international researchers, faculty, and staff prior to issuing visa documents;
4. Provide a point of contact for export issues; and
5. Appropriately staff roles required to support users and locations impacted by export controls.

6.5 Principal Investigators: Individuals approved by Saint Louis University as Principal Investigators shall:

1. Read and understand the information on export controls provided by the Export Control Officer;
2. Before beginning any research, determine whether any export control issues may apply to the project;
3. If applicable, respond to export control questions in eRS in an appropriate manner;

4. Contact the Export Control Officer for help to determine if export controls and/or licenses must be obtained;
5. Work with the Export Control Officer to establish a Technology Control Plan prior to beginning export controlled research;
6. Have an approved Technology Control Plan in place prior to requesting the release of funds by the Office of Sponsored Programs Administration;
7. Ensure that no export controlled data or technology is included in open presentations or publications by project personnel; and
8. Ensure that all project personnel on the Technology Control Plan have been trained for export controlled research.

6.6 Travelers: Individuals traveling internationally on University business shall:

1. Make contact with University Export Control Officer to verify travel destination does not require license;
2. Verify with Export Control Officer that University equipment/information being taken is authorized to be taken to destination; and
3. Fill out and return Temporary Export Certificate prior to leaving for trip.

6.7 Research Administration shall:

1. Maintain eRS or comparable system, that allows clinical trials and proposals to be uploaded and reviewed;
2. Provide a point of contact for export issues; and
3. Appropriately staff roles required to support users and locations impacted by export controls.

7.0 PROCEDURES

7.1 Notification and Management

A PI and/or the supervising department or unit must contact the Export Control Officer as soon as possible if any of the following occur:

1. Any request is received for information from a representative of the U.S. government regarding export controlled items, data, and/or export licenses.
2. A shipment from or to the University is detained or seized by U.S. Customs.
3. A subpoena or other criminal procedure notification related to U.S. export or import laws and regulations is received.
4. A violation of export control laws or regulations, or University export control policies is suspected.

7.2 Obtaining a license

When a license is required, the Export Control Officer will coordinate the submission of a license. Obtaining a license is a lengthy and costly process. The cost of obtaining an export license is the responsibility of the Principal Investigator.

If the Export Control Officer determines that the University must apply for a license, the work listed on the license application will not be conducted until a license is in place.

In the event that it is not possible to obtain a license or to control the export of technologies via a TCP, it may not be possible to accommodate the proposed research at the University. In such cases the Export Control Officer in conjunction with the Vice President and General Counsel will make the final determination on whether or not a project may be conducted at the University.

8.0 SANCTIONS

(1) External Sanctions

Violations of export control laws and regulations can result in civil and criminal penalties for both individuals and the University. Penalties apply to each individual violation, with a single project possibly incurring multiple violations. Civil penalties include fines of up to \$250,000 for each violation, and may also include a denial of export privileges, loss of the ability to contract with the federal government, and the seizure and forfeiture of the goods involved in the transaction. Criminal penalties may be imposed with up to a \$1 million fine and/or up to 20 years imprisonment against the individual for each violation. Most enforcement actions are made public by the government.

(2) Internal Sanctions

Individuals who fail to comply with this policy and procedures associated with it will be subject to disciplinary actions. Non-compliance can result in suspension or termination of research, and/or a report of suspected misconduct and/or violation reporting to government regulatory agencies. Disciplinary action will be guided by the University's Faculty Manual, Staff Handbook, or student guidelines as appropriate.

This Policy does not limit the University's ability to impose greater sanctions or impose immediate action against serious violations. Disciplinary actions appropriate to the severity of the infraction will be carried out as needed.

9.0 CHANGES TO THIS POLICY

Changes to this policy may be necessary from time to time. At a minimum the policy and all other program policies, procedures and guidelines will be reviewed on an annual basis.

10.0 REFERENCES

Department of State: *International traffic in Arms regulations (ITAR) 22 CFR §§ 120-130*
The United States Munitions list; 22 CFR 121

Department of Commerce: *Export Administration Regulation (EAR) 15 CFR §§ 730-774*
Commerce control list “Dual-use” Items list; 15 CFR 774

Department of the Treasury: *Foreign Assets Control Regulations (FACR) 31 CFR §§*
500-599

National Security Decision Directive 189 (NSDD 189) *National Policy on the*
Transfer of Scientific, Technical and Engineering Information 21 SEP 1985

Ribicoff Amendment to the 1976 Tax Reform Act (TAR) *26 USC 999; Associated*
Regulations 26 CFR 7.991

POLICIES RESCINDED

- Export Control Policy RC-003, Version 2.0, September 1, 2013

APPROVAL SIGNATURE

This policy was approved by:

William Kauffman
Vice President and General Counsel

Date

REVISION HISTORY

EFFECTIVE DATE	VERSION NUMBER	MODIFICATION
05/11/2016	1.0	New