SAINT LOUIS UNIVERSITY

Export Control Policy (Research)

Policy Number: RC-003  
Version Number: 2.0
Classification: Research Compliance  
Effective Date: September 1, 2013
Responsible University Official: Vice President for Research

1.0 INTRODUCTION

The free and unhampered pursuit and communication of knowledge and truth is essential to the purpose of a university. Saint Louis University is committed to the academic freedom to publish and disseminate the results of research and other academic activities as a means to fulfill its mission. It is the policy of Saint Louis University that its instruction, research, and public service missions are to be accomplished openly and without prohibitions on the publication and dissemination of the results of academic and research activities. Research or other activities that restrict open dissemination will be accepted only with the approval of the Vice President for Research and after careful scrutiny for Export Controls or other issues.

2.0 PURPOSE

The purpose of this policy is to ensure, to the greatest extent possible, that the University and its researchers are able to freely and openly disseminate the results of their research. Export control regulations inherently restrict this academic freedom. If classified or sensitive research is accepted by the University, steps must be taken to ensure that the benefits to society outweigh the commitment to open access. The University and its researchers must be in 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 Targeted Economic Sanctions Program (OFAC). (See Appendix A).

3.0 APPLICABILITY

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

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 including laptops, mobile phones, and portable storage devices.

Export control regulations apply whether or not the activity or technology is funded by a grant, contract, or any other type of agreement, and whether or not there is a citation of the EAR or ITAR in the award documents. The sponsorship of a project by any agency of the U.S. government does not mitigate, supersede, or remove the University's responsibility to comply with federal export control laws. Sponsorship of research or other activities by any agency of the Department of Defense must be closely screened for export controls restrictions.

4.0 POLICY

It is the policy of Saint Louis University and its mission to encourage academic freedom and the ability to openly and freely disseminate research and the results thereof. Research and other activities that are considered classified, proprietary, or sensitive may restrict open dissemination and therefore are contrary to the University's commitment to open access. For reasons of national security and/or protection of trade, certain activities within the research enterprise are subject to U.S. export control laws and regulations. Classified or restricted projects will be supported by Saint Louis University only after it has been determined that the benefits of the project outweigh the loss of open dissemination of the research. The Vice President for Research will make this determination. Researchers must understand and agree to any loss of academic freedom associated with restricted research before it will be accepted.

Export control regulations are complex and violations can result in severe civil and criminal penalties, including fines and/or imprisonment. While much of university research is excluded from export controls regulations, Saint Louis University must ensure that its investigators perform their research in compliance with governmental laws and regulations. All University faculty, staff, students, and visiting scholars are expected to follow the procedures which are attached to this policy as they pertain to restricted research. 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.

For specific procedures and guidance in complying with Export Control regulations and University policy, please see the following Appendices:

- Appendix A: Regulations covering Export Controls
- Appendix B: Definitions
- Appendix C: Guidelines and Procedures, Prior to Submission of Applications
5.0 NON-COMPLIANCE

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 against the University and a fine up to $250,000 and/or up to 20 years imprisonment against the individual for each violation. Most enforcement actions are made public by the government.

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

6.0 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 CFR730-774 Commerce control list “Dual-use” Items list; 15 CFR 774

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


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

7.0 POLICIES RESCINDED

Export Control Policy, Version 1.0, August 26, 2010.
8.0 APPROVAL SIGNATURES

This policy was approved by:

SIGNED BY RAYMOND C. TAIT, Ph.D.  08/27/2013

Raymond C. Tait, Ph.D.
Vice President for Research
Saint Louis University

Date

VERSION HISTORY

<table>
<thead>
<tr>
<th>EFFECTIVE DATE</th>
<th>VERSION NUMBER</th>
<th>MODIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 AUG 2010</td>
<td>1.0</td>
<td>New</td>
</tr>
<tr>
<td>01 SEPT 2013</td>
<td>2.0</td>
<td>Revision</td>
</tr>
</tbody>
</table>
APPENDIX A
TO
EXPORT CONTROLS POLICY, RC-003
EXPORT CONTROLS REGULATIONS

The federal export control regulations are complex and violations can result in severe civil and criminal penalties. It is important that all members of the University understand their obligations under these regulations and promote compliance. There are three primary sets of regulations covering export controls:

1. Commerce Department Export Administration Regulations (EAR): 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 (CCL). 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 (ITAR): 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) and space items and associated systems and equipment (even if not for military 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).


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.

------

Other federal agencies have authority relevant to export controls on certain types of items and technologies, such as the following:

- Department of Energy (nuclear technology, high-energy lasers, etc.) (10 CFR 810);
- Department of the Interior, Fish and Wildlife Service (endangered species) (50 CFR 17);
- Department of Justice, Drug Enforcement Administration (drugs of abuse, chemicals, and precursors) (21 CFR 1311-1313);
- Nuclear Regulatory Commission (nuclear equipment and materials) (10 CFR 110);
- Food and Drug Administration (pharmaceutical development and medical devices) (21 USC 301; 21 CFR 312.1106).
APPENDIX B
TO
EXPORT CONTROLS POLICY, RC-003
DEFINITIONS

Deemed Export: Release of technology or source code subject to export control regulations to a foreign national in the United States. Such a release is "deemed" to be an export to the home country of the foreign national under the EAR.

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.

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 for Research 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 oral, written, electronic, or visual disclosure, shipment, transfer, or transmission outside the United States to anyone, including a U.S. citizen, of any commodity, technology (information, technical data, or assistance), or software code.

Foreign National: Any individual that is not a U.S. Person. "Foreign National" can also include any business, organization, or entity not licensed to do business within the borders of the United States.

Fundamental Research: Basic and applied research in science and engineering performed or conducted at an accredited institution of higher learning in the United States where the resulting information is ordinarily published and shared broadly within the scientific community (see National Security Decision Directive 189).

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: Specific information necessary for the development, production, or use of a good, but not the good itself.
**U.S. Person:** A citizen of the United States, a lawful permanent resident of the United States, or a protected individual (e.g., refugees or persons seeking asylum) as defined in 8 U.S.C. 1324b(a)(3).

**Use:** Operation, installation (including on-site installation), maintenance (checking), repair, overhaul, or refurbishing.
APPENDIX C
TO
EXPORT CONTROLS POLICY, RC-003
GUIDELINES AND PROCEDURES, PRIOR TO SUBMISSION OF APPLICATION

Prior to submission through eRS, PI’s must clear the project through the University’s Office of Research Integrity (ORI). PI must complete the eRS transmittal form and answer the export controls questions accurately.

I. Identify research project re: export controls
   a. Any foreign nationals involved?
   b. Any foreign entities/institutions involved?
   c. Any travel to foreign countries for the project?
   d. Shipping, sending, faxing, emailing information or items abroad?
   e. Is the sponsor an agency of the Department of Defense?
   f. Any restrictions on publication/presentation of research?
   g. Any restrictions on foreign nationals working on project?

II. If yes to any of the above questions, PI must contact the Office of Research Integrity and provide the following information:
   a. List of names and institutional affiliation of all foreign nationals involved
   b. Specific list of items/software/technology involved
   c. List of places abroad to be visited for the research
   d. Copy of work plan, proposal, or request for proposal/application

III. ORI will screen for compliance
   a. Entities and personnel
   b. Items/software/technology
   c. Work plan
   d. Countries/cities to be visited
      i. Any embargoed countries listed?

IV. ORI will determine if research is exempt from export controls
   a. Fundamental Research
   b. No controlled items involved
   c. No individuals on denied persons list
   d. License exemptions

V. ORI will determine if Technology Control Plan (TCP) is needed
   a. Complete form with PI
      i. IT assist with technical security
   b. Ensure all individuals sign
   c. Conduct training
   d. Copies of signed TCP to OGC-Research Compliance

VI. If research is considered export controlled and requires a license, PI must:
   a. Contact Vice President for Research for opinion on whether the research can be done at SLU
   b. If license is required, provide information on how license fees will be paid.
   c. Secure information, research findings, data, equipment, etc., according to license and TCP.
d. When license is received, conduct research accordingly.

VII. OGC-Research Compliance will periodically review TCP with PI, Office of Research Integrity, etc.
APPENDIX D
TO
EXPORT CONTROLS POLICY RC-003
PROCEDURES FOR EXPORT CONTROLLED RESEARCH

Administration

It is the intent of the University to maintain compliance with federal export controls while preserving the open academic environment to pursue fundamental research (see National Security Decision Directive 189) and educational exclusions to export controls. Under the Fundamental Research Exclusion, the majority of University research projects can be conducted without export control restrictions. However, members of the research community must not assume their activities are exempt. The fundamental research exclusion does not cover research activities performed outside the United States, and certain activities and information (See Appendix A).

The Vice President for Research is the Empowered Official at Saint Louis University responsible for the ultimate management and control of the export controls policy. The Office of Research Integrity, under the direction of the Associate Vice President for Research, 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 Office of the General Counsel, Information Technology Services, Division of Business and Finance, Human Resources, Office of International Services, and the Office of University Compliance.

The Vice President for Research has the authority to deny application for or acceptance of any award for which the University’s commitment to open access and full disclosure of research activities is compromised.

Responsibilities:

Office of Research Integrity shall:

- Establish, maintain and publish policies and procedures to ensure compliance with export control laws and regulations;
- Monitor research proposal submissions in order to screen projects, people, and entities for activities involving embargoed or sanctioned countries, organizations, and/or individuals.
- Facilitate the preparation of technology control plans;
- Periodically review active Technology Control Plans, in collaboration with Information Technology Services and the Office of the General Counsel/Research Compliance to verify that the plans are being properly followed regarding the federal export control regulations and this policy;
- Provide staffing to serve as liaison with University employees concerning export controls;
- Design and implement an export controls training program for faculty, staff, and students engaged in research at the University. Recommend or require training for specific situations involving export controls;
• Document and maintain export control training in accordance with any applicable federal guidelines or record keeping; and
• Notify the appropriate federal agencies of export control violations in a timely manner.

Office of University Compliance shall:

• Serve as the point of contact for calls made to the compliance hotline regarding export control issues;
• Notify ORI and coordinate the investigation of concerns conveyed through the hotline or other means regarding suspected violations of export control regulations and University policy; and
• Ensure the Vice President for Research is notified of the findings from all reviews and investigations related to export controls.

Human Resources shall:

• Provide (or make available) to the Compliance Administrator in the Office of Research Integrity a report of foreign nationals who are newly hired or who transfer positions within the University on a monthly basis.

Information Technology Services shall:

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

Office of International Services with the University Registrar shall:

• Facilitate access for the Office of Research Integrity (ORI) to reports listing all international students enrolled at Saint Louis University at least once every semester (Fall, Spring, Summer);
• Provide a listing of current visiting faculty and staff, including researchers, to ORI at least once every six (6) months;
• Provide ORI with a listing of potential international researchers, faculty, and staff prior to issuing visa documents;
• Provide a point of contact for export issues; and
- Appropriately staff roles required to support users and locations impacted by export controls.

**Principal Investigators:** Individuals approved by SLU to be Principal Investigators are required to:

- Read and understand the information on export controls provided by the Office of Research Integrity (ORI);
- Before beginning any research, determine whether any export control issues may apply to the project;
- Contact the Office of Research Integrity for help to determine if export controls apply and if licenses must be obtained;
- Work with the Office of Research Integrity to establish a Technology Control Plan prior to beginning export controlled research;
- Have an approved Technology Control Plan in place prior to requesting the release of funds by the Office of Sponsored Programs;
- Ensure that no export-controlled data or technology is included in open presentations or publications by project personnel; and
- Ensure that all project personnel on the Technology Control Plan have been trained for export controlled research.

**Procedures**

Projects that fall under the federal export controls exclusions (See Appendix B and Appendix C) may be accepted by the University as long as the appropriate exclusion is not negated. For example, elimination of the Fundamental Research Exclusion occurs if any restriction of publication or restriction of access by foreign personnel to the research or research results is part of the project.

Projects involving any of the following must be reviewed by the Office of Research Integrity:

- Restrictions on publication, presentation, or sharing of results openly;
- Restrictions on foreign nationals working on the project;
- Shipping tangible items outside the United States;
- Sharing proprietary, confidential, or restricted information or software code with foreign nationals within the United States or abroad;
- Interactions with embargoed or sanctioned countries, organizations, or individuals (Restricted Parties) (including purchases from foreign suppliers);
- Travel to a foreign country with controlled technologies including laptops, mobile phones, and portable storage devices.

If a project involves any of the aforementioned export activities, the Vice President for Research must determine if the research project is acceptable to the University and conforms to its commitment to open access and academic freedom.

If export controlled research is accepted, the University must:
• Assist the researcher in obtaining an export license and document the process; or
• Determine that no export license is required; or
• Determine that while an export license is required, an exception or exemption to the requirement(s) exists; and
• Ensure that the research and its findings are secured in accordance with federal regulations with a Technology Control Plan.

The University must document each determination.

Certain events regarding export controls require University personnel to immediately notify the Office of Research Integrity and the Office of General Counsel. A PI and/or the supervising department or unit must contact the Office of Research Integrity and the Vice President for Research as soon as possible if any of the following occur:

• Any request is received for information from a representative of the U.S. government regarding export controlled items, data, and/or export licenses.
• A shipment from or to the University is detained or seized by U.S. Customs or other government agency. A subpoena or other criminal procedure notification related to U.S. export or import laws and regulations is received. University Personnel may not, under any circumstances, interfere with or impede any federal law enforcement officer performing his/her official duties.
• A violation of export control laws or regulations, or University export control policy is suspected.

Procedure for Obtaining a License

As the empowered official, the Vice President for Research is the signature authority for export control license applications. In instances where a license is required and the project is determined to be acceptable as an exception to University policies, the Office of Research Integrity 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 an export controls license is required, no work under a related contract or grant may begin until the process is complete and a license is issued.

In the event that it is not possible to obtain a license or to control the export of technologies via a Technology Control Plan (TCP), it may not be possible to accommodate the proposed research at the University. In such cases the Vice President for Research will determine that the project may not be conducted at the University.

Security and Technology Control Plans

All SLU department's 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 PI or department takes possession of controlled items, a Technology Control Plan (TCP) must be in place (see Appendix D).

The purpose of a TCP is to protect export controlled technology which is not covered under exclusion or 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 project personnel listed on the TCP must be screened by the Office of Research Integrity. The finalized TCP shall be reviewed and approved by the University Empowered Official or his/her designee for export controls. 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 when a new member of the research team has been approved, and/or if the scope of work 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 TCF 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.

Documentation Retention

Principal Investigators must keep electronic or hard copies of all export documentation including financial records and shipping documentation (e.g., FedEx forms, commercial invoices, purchase orders, etc.) and University export certification documents in their research 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.

Internal Reviews

Regular internal review of files is required in order to ensure proper practices and procedures by persons reporting to senior management.

Training Requirements

Researchers must complete export controls training as presented by the Office of Research Integrity before beginning work on any EAR or ITAR controlled project.
APPENDIX E
TO
EXPORT CONTROLS POLICY RC-003
EXCLUSIONS FROM EXPORT CONTROLS

The EAR and ITAR specifically exclude or exempt certain types of information and data from the scope of regulatory oversight. These exclusions and exemptions ensure that the majority, but not all, of the University research and instructional activities are not subject to export control, or if controlled, do not require licensing. The exclusions most commonly applicable to University research and instruction are:

1. **Fundamental Research Exclusion (FRE)**
The exclusion of fundamental research from export controls stems from National Security Decision Directive 189 (NSDD 189). NSDD 189 defined fundamental research as:

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.

Both the EAR and ITAR have provisions for a Fundamental Research Exclusion (FRE), which applies to most research conducted at the University. The regulations exclude fundamental research from deemed export controls. Under the FRE, export licenses and other government approval are not needed in order to involve foreign nationals (non US persons) to participate in research at the University in the United States.

University research will not be deemed to qualify as fundamental research if:

(1) the University accepts any restrictions on the publication of the information resulting from the research, other than limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by sponsor or to insure that publication will not compromise patent rights of the sponsor (per EAR; even limited review for proprietary reasons eliminates the FRE under ITAR); or

(2) the research is federally funded and specific access and dissemination controls regarding the resulting information have been accepted by the University or the researcher.

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 Information 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 U.S. 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 Directorate of Defense Trade Controls (DDTC).

   The application of this exemption is more limited than the FBE 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.
APPENDIX F

TO

EXPORT CONTROLS POLICY RC-003

ACTIVITIES AND INFORMATION NOT COVERED BY

FUNDAMENTAL RESEARCH EXCLUSION

Certain activities and information are not covered by the fundamental research exclusion and remain subject to the export control laws and regulations including:

- **Sharing of Information and Deemed Exports**
  - Fundamental research may usually proceed openly and be shared freely with a foreign person in the United States without constituting a deemed export. Sharing export controlled items, source code, or technical know-how of regulated information or research with foreign nationals who do not have a federal license to access information or research is prohibited.

- A technical assistance agreement to provide training to foreign nationals by U.S. citizens or permanent residents where controlled technology is involved requires an export license.

- **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 Office of Research Integrity to obtain an export control determination and develop a technology control plan 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 Compliance Administrator in the Office of Research Integrity**. An example of this would be if a PI receives an unexpected email containing information believed to be export controlled.

- **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 Office of Research Integrity.

**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 Compliance Administrator in the Office of Research Integrity 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.

**Travel Abroad**
International travel to meetings, seminars, and other professional events outside the U.S. may be subject to licensing requirements. Special attention should be given by those traveling with laptops, mobile phones, and portable storage devices. SLU 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 SLU 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 restricted, sanctioned, or embargoed countries are responsible for notifying the Compliance Administrator in the Office of Research Integrity who will work with the individual to determine whether approval or licenses are necessary. If necessary, SLU 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 U.S..

**Confidentiality Agreements and Nondisclosure Agreements**
In order to maintain the fundamental research exclusion (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.

A third party or funding sponsor may ask for a formal agreement such as a Confidential Disclosure Agreement (CDA) 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 (ORDS) and the Office of Sponsored Programs Administration (SPA). If an agreement refers to export controls, it will also be reviewed by the Office of Research Integrity. These offices have signature authority to bind the University in such agreements. An individual researcher cannot sign such agreements on behalf of the University.

In some cases a researcher may be asked by a sponsor or third-party to sign a CDA or NDA as part of an ongoing or proposed project such as a clinical trial or potential project. Individual researchers must not sign any such document and immediately contact ORDS.

Researchers must not enter into any informal “side deals” with sponsors to limit the discretion of the researcher(s) to publish or disseminate research findings (e.g., promising to hold off on the submission of an article to a publisher until the sponsor approves). Such agreements have the potential to nullify the fundamental research exclusion.
APPENDIX G
TO
EXPORT CONTROLS POLICY RC-003

Technology Control Plan (TCP)
For
Export-Controlled Technology/Information

This project has been identified as involving or potentially involving technology/information that is export controlled under the purview of either the State Department’s International Traffic in Arms Regulations (ITAR) or the Department of Commerce’s Export Administration Regulations (EAR). Links to information about ITAR (22 CFR 120-130) and EAR (15 CFR 730-774) as well as the University Export Control Policy (RC-003) can be found on the University Division of Research Administration website.

It is unlawful under the ITAR and EAR to transfer any export controlled items, information, or software to any non-U.S. persons (foreign persons or entities) inside or outside the U.S. without proper authorization (e.g., license or documented exclusion/exemption). The Export Control Regulations (EAR and ITAR) require that a Technology Control Plan (TCP) be in place to prevent unauthorized export or transfer of controlled items, materials, information, or technology.

Since this project has been identified, technical information, data, materials, software, or hardware, (i.e., technology used in this project) must be secured from use, access, and possible observation by unlicensed non-U.S. persons. University Policy RC-003 requires that all SLU departments that possess export controlled items are responsible for providing and maintaining the appropriate security of controlled items and related documentation. Security measures will be appropriate to the classification involved.

Before a department obtains controlled items, a Technology Control Plan (TCP) must be in place. This document is the base template for the minimum elements of a TCP. Establishing a TCP is a multi-step process and two-part form. It is the responsibility of the Principal Investigator (PI) to develop a written TCP which must be approved and signed by Carole Knight, Ph.D., Associate Vice President for Research and Director Office of Research Integrity. The PI must ensure each person working on the project has read and understands the information presented in this briefing and the TCP. In addition, Office of Research Integrity staff may meet with project personnel regarding the handling of Export-Controlled Technology/Information and the TCP. Project personnel must sign the TCP Certification before they can begin work on the project. The signed TCP and TCP Certification should be returned to Todd Richardson, Ph.D., Compliance Administrator, Office of Research Integrity at Fusz Memorial Hall Suite 261. Copies of the signed TCP and TCP Certification will be sent to the PI and the Office of University Compliance. Periodic audits of the TCP will be conducted, and amended when a new member of the research team has been approved, or if the scope of work changes.

For assistance with this form, please contact Todd Richardson, Ph.D., Compliance Administrator in the Office of Research Integrity at 314-977-2262 or trichar@slu.edu
TECHNOLOGY CONTROL PLAN

In accordance with export control regulations as specified in EAR and ITAR, a Technology Control Plan is required for this project in order to prevent unauthorized export of controlled technology deemed to be sensitive to national security or economic interests. This form contains the basic and minimum elements of the TCP.

<table>
<thead>
<tr>
<th>Date:</th>
<th>Title of Research Project/Activity:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Is this project/activity Sponsored? (i.e., funded)  
Yes [ ]  No [ ]

Related eRS Proposal Number(s):
Related University Fund Number(s):

Technical description of item, technology, equipment; software to be controlled:

Export Classification  
ECCN:  
ITAR Category:

Principal Investigator:  
Department & Address:

Phone:  
E-mail:

1. Physical Security Plan: (Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratories, or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of "work-in-progress" and protecting physical items.)

   a. Location: (Describe the physical location of EACH sensitive technology/item to include building and room numbers. A schematic of the immediate location is highly recommended.)

   

   b. Perimeter Security: (Describe perimeter security features of the location of the protected technology/item.)

   

   c. Physical Access Security: (Provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access, e.g., secure doors, limited access, security badges; etc.)

   

   d. Item Marking: (Describe your plan for identifying items that are export controlled. Export controlled information must be clearly identified and marked as such, e.g., "Export Controlled – Do Not Distribute to Non-U.S. Persons").

   

   e. Item Storage: (Describe your plan for protecting the physical technology and/or by-product. Both soft and hard copy data, notebooks, reports, and research materials are stored in locked cabinets; preferably in rooms with key-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing "export controlled" technology are to be physically secured from unauthorized access.)

   

   f. Item Destruction/Return: (Describe how the export controlled items will be handled at the end of the project or when they are not needed anymore; e.g., shredding, file wipes, destroying hard drives, return to sponsor; etc.)

   

2. Information Security Plan: (Appropriate measures should be taken to secure controlled electronic information, including User ID's, password control, SSL or other approved encryption technology. Database access must be managed via a Virtual Private Network (VPN),

Appendix G, Export Controls Policy  
Effective Date: September 1, 2013
allowing only authorized persons to access and transmit data over the Internet, using 128-bit SSL or other advanced, federally approved encryption technology.

a. **Structure of IT security:** (Describe the information technology [IT] setup/system at each technology/item location)

   ▶

b. **IT Security Plan:** (Describe in detail your security plan, i.e., password access, firewall protection plans, encryption; etc.)

   ▶

c. **Verification of Technology/Item Authorization:** (Describe how you are going to manage security on exported controlled technology in case of termination of individuals working on new projects; etc.)

   ▶

d. **Conversation Security:** (Describe your plan for protecting information about controlled technology in conversations. Discussions about the project or work product are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third-party subcontractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.)

   ▶

3. **Project Personnel:** (Clearly identify every person, including their national citizenship, who is determined to have authorized access to the controlled technology. It is the responsibility of the PI to inform the Office of Research Integrity of any new addition to the project personnel. The TCP will be updated accordingly.)

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Country of Citizenship</th>
<th>Job Title/Work Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. **Personnel Screening Procedures:** (At a minimum, all persons that may have access to exported controlled materials or data must be listed on the TCP and screened against government restricted persons/entities lists. Restricted Parties Screening [RPS] will be completed by the Office of Research Integrity.)

   a. **RPS Results:** (Provided by Office of Research Integrity.)

      ▶

   b. **Additional Checks:** (Describe any other screening procedures, e.g., criminal, driver’s license, SF-85, SF-86; etc.)

      ▶

5. **Training/Awareness Program:** (Researchers must complete export controls training before beginning work on any EAR or ITAR controlled project. The Office of Research Integrity shall recommend or require training for specific situations involving export controls. PIs are responsible for ensuring that all project personnel listed on a TCP have been trained on controlled research.)

   a. **Basic Training:** (All project personnel listed on a TCP must receive mandatory basic training on export controls provided by the Office of Research Integrity prior to using any export controlled items or technology. List the name of all project personnel along with their banner number and the date they completed mandatory basic training on export controls provided by the Office of Research Integrity.)

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Banner #</th>
<th>Basic EC Training Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Appendix G, Export Controls Policy   Effective Date: September 1, 2013   Page 3 of 8
b. **Additional Training:** (Describe training for project personnel about the restrictions and security measures specific to this project at the controlled technology/items. Include information on how you will maintain awareness of the applicable export control, TCP, and University Export Controls Policy.)

6. **Compliance Assessment Program:** (Ongoing compliance monitoring is required by the export control regulations. PIs must conduct periodic (at least annually) internal self-evaluations of this TCP and report any findings to the Office of Research Integrity. In addition to self-evaluation, the Office of Research Integrity and/or the Office of University Compliance may conduct periodic evaluations and/or training to assess compliance with the TCP procedures. Any changes to the approved procedures or personnel having access to export controlled information covered under this TCP must be cleared in advance by the Office of Research Integrity. Authorized personnel should contact the Office of Research Integrity if there are any questions or concerns related to this TCP.)

   a. **Self-Evaluation Schedule:** (Describe how often you plan to review/evaluate your TCP. Plans must be re-evaluated at least annually.)

   b. **Action Item and Corrective Procedures:** (Describe your process to address findings in your self-evaluation audits.)

7. **Project Termination:**

Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect the export controlled items and/or technical data unless earlier terminated, or when the technical data has been destroyed or determined to be no longer export-controlled. Disposition of export controlled equipment, software, and technical data upon project termination shall be coordinated with the Office of Research Integrity. All records pertaining to the export of export controlled items and technical data shall be retained in accordance with University policy (RC-003) and applicable federal regulations.

8. **Acknowledgements and Certifications**

**Principal Investigator:**

I certify that I have read the above information submitted in this Technology Control Plan, that such information is accurate and correct to the best of my knowledge and belief, and that I will implement this project in a manner consistent with this plan and in compliance with all applicable export control regulations and University Policy. Furthermore, I recognize that the implementation of this Technology Control Plan is my responsibility, and I will contact the Office of Research Integrity if any changes occur to my research and/or to address questions I have regarding the designation, protection, or use of export-controlled technology/information.

---

**Signature**

**Date**

**Printed Name**

**Department Chair:**

I acknowledge that I have received this document after it was completed by the principal investigator. Based on information provided herein by the principal investigator, I approve of this Technology Control Plan with the

**Appendix G, Export Controls Policy**

**Effective Date:** September 1, 2013
understanding that the principal investigator will be responsible for acting in compliance with the plan once it has been approved by the Empowered Official or his designee.

________________________________________________________________________
Signature Date

________________________________________________________________________
Printed Name

Dean:

I acknowledge that I have received this document after it was completed by the principal investigator. Based on information provided herein by the principal investigator, I approve of this Technology Control Plan with the understanding that the principal investigator will be responsible for acting in compliance with the plan once it has been approved by the Empowered Official or his designee.

________________________________________________________________________
Signature Date

________________________________________________________________________
Printed Name
9. Research Administration Review and Approval

Compliance Administrator:
I certify that I have received this signed Technology Control Plan from the principle investigator.

Date TCP
Received:

__________________________
Signature                        Date

__________________________
Printed Name

Empowered Official:
I acknowledge that I have received and reviewed this Technology Control Plan. I approve this Technology Control Plan and direct the above listed principal investigator to implement it accordingly. I direct the Office of Research Integrity to monitor the implementation of this TCP and the associated project(s) in order to ensure compliance with all applicable export control laws and regulations as well as University Policies.

Date TCP
Received:

__________________________
Signature                        Date

__________________________
Printed Name
TECHNOLOGY CONTROL PLAN CERTIFICATION

Principal Investigator: __________________________________________

Department: __________________________________________________

Sponsor Name: _________________________________________________

Project Title: _________________________________________________

This is to acknowledge I have read and understand the Technology Control Plan (TCP) for the project listed above, that I have discussed the procedures with the PI, and I agree to comply with the requirements of the TCP. If I have any questions about this TCP, its requirements, or following any procedure, I will contact the PI for advice before proceeding. I understand that the PI has agreed to update this plan as required and as personnel are added to or deleted from this project.

Signature Date
Printed Name/Role

Signature Date
Printed Name/Role

Signature Date
Printed Name/Role

Signature Date
Printed Name/Role

Signature Date
Printed Name/Role

Signature Date
Printed Name/Role

Acknowledgement of Principle Investigator:

Signature Date
Printed Name/Role
Signed TCP Certification must be returned to Todd Richardson, Ph.D., Compliance Administrator, Office of Research Integrity, 3700 West Pine Mall, Fusz Memorial Hall Suite 261, St. Louis, MO 63108. Contact: 314.977.2262 or exportcontrols@slu.edu

TCP Reviewed and Certification Received:

Signature                                      Date

Printed Name/Role

Appendix G, Export Controls Policy   Effective Date: September 1, 2013