International Collaborations and Export Controls

1. Introduction and Scope

USC engages in a variety of activities related to research, instruction, healthcare, student outreach, and other strategic partnerships and affiliations that may create obligations under United States export control regulations, the Foreign Corrupt Practices Act (FCPA), and economic and trade sanctions regulations. This policy describes the laws and university procedures that apply to these activities and interactions. It is divided into sections applicable to:

- Research and teaching
- International travel
- Doing business with international partners
- Restrictive trade practices and boycotts

2. Background

2.1 Export Controls: Export controls are federal laws that regulate the export of sensitive technologies, equipment, software, biological agents and related data and services. Two sets of export control regulations are most frequently encountered in the context of university research, teaching, and international travel. The Commerce Department regulates exports of commercial items with potential military applications (so called "dual-use" items) under the Export Administration Regulations ("EAR"). The State Department regulates exports of items and services specifically designed for military applications under the International Traffic in Arms Regulations ("ITAR").

Under these regulations, specific licenses may be required for exports of these items (e.g., defense articles, items with potential military applications, select agents), depending on their export classification, the destination country, and their intended end use. These regulations also restrict "deemed exports" of controlled technology and software source code to foreign nationals within the United States, as such releases are deemed to be exports to the foreign national's home country.

2.2 Foreign Corrupt Practices Act (FCPA): The Foreign Corrupt Practices Act (FCPA)(15 United States Code (U.S.C.) Section 78dd-1, et seq.) was enacted in 1977 in response to revelations of widespread bribery of foreign officials by U.S. companies in order to win business. The anti-bribery provisions of the FCPA generally prohibit U.S. organizations and employees from offering payments or anything of value to foreign officials to secure an improper advantage or obtain or retain business.

The U. S. Department of Justice (DOJ), the government agency charged with enforcing the FCPA, requires that all United States entities exercise due diligence in the selection of foreign business partners, and closely scrutinize entities who exhibit red flags that increase the likelihood that a payment to the entity may violate FCPA requirements and limitations. See the "Doing Business with International Partners" section of this policy for additional detail.

2.3 Economic Sanctions: Under federal regulations administered by the Office of Foreign Assets Controls (OFAC) in the Department of Treasury, the U. S. imposes economic and trade sanctions against targeted foreign countries and their governments, as well as specified entities and individuals for reasons of national security and foreign policy. Where it has imposed comprehensive sanctions on a country, virtually all trade is prohibited and travel is restricted. Even if sanctions are limited, trade and travel restrictions are likely to be significant. Consult Section 3.14 of this policy for additional detail.

3. Policy

3.1 The university and all of its employees and students must comply with applicable export control, economic and trade sanctions, and anti-bribery and corruption laws in all university activities, as well as the additional provisions set forth below.

Research and Teaching

3.2 "Fundamental Research": USC generally does not accept research projects that have restrictions on the dissemination of research results, or that attempt to restrict participation in the research on the basis of nationality, unless an exception has been approved under Section 4 of this policy. University-based research projects without these restrictions are considered to be "fundamental research" under National Security Decision Directive (NSDD) 189 and are exempt from export control requirements.

3.3 Information in the Public Domain: In addition to "fundamental research", if information has already been published or is within the public domain, it is generally not subject to export control regulations and may be disseminated freely without considering possible export licensing requirements. Under export control regulations, information is "published" or within the "public domain" when it becomes accessible to the public in any form, including:

- Publication in periodicals, books, print, electronic or other media available for general distribution (including websites that provide free uncontrolled access) or for distribution to a community of persons interested in the subject matter, such as those in a scientific or engineering discipline
- Readily available at libraries open to the public
- Patents and published patent applications available at any patent office
- Release at an open conference, meeting, seminar, trade show or other open gathering

If, however, the information enables the creation of an item that the State Department deems is covered by the ITAR, which includes items specifically designed for military applications, the information may still be export-controlled, even though it is in the public domain.

3.4 Teaching: Under export control regulations, a faculty member who is sharing information concerning general scientific, mathematical, or engineering principles that are commonly taught or released by USC as part of normal instruction in a catalog course or in an associated teaching laboratory may do so without restriction. In addition, a faculty member may freely disclose information that has already been published or is in the public domain.

3.5 Exceptions to Fundamental Research: In limited circumstances USC will accept restrictions on dissemination of research results, pre-publication review or access to a research project based on nationality. If USC accepts such restrictions – beyond limited (e.g., 30-90 days) sponsor-imposed delays to protect intellectual property rights or ensure against inadvertent disclosure of proprietary information – the related research will likely no longer be considered "fundamental research" under export control regulations. If research does not qualify as "fundamental research", complying with export control regulations and this policy may involve:

- Limitations on where the research can take place at USC
- Limiting foreign national access to all or part of the research
- Obtaining a license from the Departments of Commerce and/or State, as applicable, before disclosing export-controlled technology, technical data, or software source code to a foreign national in the United States (a "deemed export"), or before sending controlled items or information to a foreign country
- Implementation of a Technology Control Plan (TCP) to protect potentially export-controlled items or information
- Adhering to publication and personnel restrictions and the requirements of any university-imposed TCP (if applicable)

Principal Investigators must obtain approval to conduct research that is not considered "fundamental research" as set forth in Section 4 of this policy.

3.6 Actual Exports: All overseas shipments of materials, items, technology, software, and software source code constitute exports that may require a license or other form of governmental authorization, as described below. Overseas shipments include both shipping an item from the U.S. using a third party carrier (e.g., Fed Ex) as well as personally taking items abroad. However, not all exports require specific governmental authorization. Examples of actual exports include:

- Ordering or sending equipment, tools, software, or other items in order to conduct research in another country
- Conducting research which involves the physical shipment of a product internationally

- Shipping or bringing controlled items in connection with a presentation, conference, seminar, course, or research in a foreign country (e.g., a prototype of an experimental laser or an infrared camera used as a data collection tool in related research)
- Taking items (e.g., laptops, software, equipment, prototypes, pathogens, toxins) overseas in connection with international travel

3.6.1 Exports that do not require a license: The following exports typically do not require governmental authorization in the form of an export license:

- Taking a data storage device (e.g., a laptop, tablet, smart phone, USB flash drive, or smart watch) with only "mass market" encryption software overseas in connection with international travel, as long as the data storage device does not also contain other software or data that is export controlled. For this purpose, "mass market" encryption items are those that are commonly sold "off the shelf" at retail stores or online (e.g., Microsoft Windows operating systems, virtual private network applications, and word processing applications with file security features).
- Taking research-related information (e.g., publications, presentations, underlying research results) abroad on projects that do not have any restrictions on publication of results or access to the research on the basis of nationality.

3.6.2 Exports that may require a license: The following exports may require governmental authorization:

- Taking a device with non-commercial, special purpose encryption software overseas in connection with international travel.
- Taking a device that contains proprietary or export controlled data.
- Shipping or taking defense articles controlled under the ITAR abroad in order to conduct research in another country. In contrast, researchers are authorized to temporarily export nearly all commercial/dual-use items subject to the EAR under a "tools of trade" exception for all destinations, except the countries subject to comprehensive economic sanctions (see Section 3.14). However, certain types of sensors such as infrared cameras, night vision equipment and inertial measurement units may be controlled under the ITAR even though these items are being used in a project without potential military application.
- Shipping or taking pathogens and/or toxins abroad in order to conduct research in another country.

Doing Business with International Partners

3.7 USC is committed to expanding its global presence through activities like international student recruitment and learning and research opportunities that take place abroad. The Office of the Vice President for Strategic and Global Initiatives must be consulted with respect to all

initiatives that involve establishment of an overseas physical presence or international research partnership with any overseas university, institution, or governmental entity.

3.8 USC employees and third party subcontractors are prohibited from directly or indirectly giving or receiving improper payments or other benefits to a foreign official to gain a commercial or other advantage in violation of the Foreign Corrupt Practices Act (FCPA). The types of payments covered by the FCPA are broad and cover anything that may confer a benefit on someone in a position to provide a commercial or other advantage to USC. Some examples include:

- Any gift of cash or a cash substitute
- Anything that is offered as a "quid pro quo" (a payment in exchange for favor or advantage)
- Any gift or entertainment that is illegal under the foreign country's laws, or known to be prohibited by the foreign official's department, agency, or organization
- Anything that may influence, or may be perceived as influencing, the decision of anyone considered to be a foreign official
- Anything given to a foreign official associated with a tender or competitive bidding process where USC is involved
- Any inappropriate entertainment (such as entertainment that is illegal under local law or U.S. law)
- Any travel, entertainment, or gifts to a family member of, or person otherwise closely associated with, a foreign official

3.9 USC faculty, staff, and student employees are expected to exercise care and take all necessary precautions to ensure that they are conducting business with reputable and qualified business collaborators (e.g., partners, representatives, recruiters, distributors and any other representatives collaborating with or on behalf of USC).

3.10 To avoid making improper payments to foreign officials when conducting university business overseas, USC faculty, staff, and student employees are also expected to perform due diligence on overseas business partners and collaborators, which can include:

- Determining whether the collaborator is qualified to perform the proposed services
- In-person interviews and visits to the collaborator's premises
- Determining whether the collaborator has personal or professional ties to a foreign government or foreign official
- Assessing the number and reputation of the collaborator's other clientele
- Evaluating the collaborators' reputation with the U.S. embassy or consulate and with local bankers, clients, and other business associates

- Determining whether the collaborator's proposed compensation is based on prevailing industry standards and is commensurate with his/her experience and the services to be rendered.

3.11 "Red flags" to be aware of include:

- Unusual payment patterns or financial arrangements (e.g., payments in cash or to a third party)
- A history of corruption in the country
- Refusal by a collaborator to accept contractual FCPA or anti-bribery language
- Unusually high commissions
- Lack of transparency in expenses and accounting records
- Apparent lack of qualifications or resources on the part of a collaborator to perform the services offered
- Whether the collaborator has been recommended by an official of a potential government customer

USC faculty, staff, and student employees should take these considerations into account when doing business with international partners, and must consult the Office of General Counsel or the Office of Compliance if there is doubt whether a proposed business partner raises FCPA concerns.

International Travel Considerations

3.12 University faculty, staff, and student employees traveling overseas must comply, as applicable, with all applicable export control and sanction regulations. This includes:

- License requirements for exports: Obtaining a license from the Department of Commerce and/or State before taking export-controlled items overseas (e.g., proprietary software source code, equipment) unless a license exception applies. See Section 3.6 ("Actual Exports").
- Economic sanctions: Adhering to any OFAC economic and trade sanctions imposed against targeted foreign countries and regimes for reasons of national security and foreign policy. See Section 3.14, below.
- FCPA considerations: Adhering to the requirements of the Foreign Corrupt Practices Act (FCPA) in all foreign financial transactions. (See "Doing Business with International Partners").

3.13 University-led Student Travel: All USC sponsored or affiliated student travel must adhere to USC's **Overseas Study Trips** policy. This includes travel: (1) under the direction of a university school or department; (2) initiated by a student-led organization affiliated with USC; and (3) travel in connection with an individual faculty member's academic or research activity.

The policy addresses USC Health Insurance for student travelers, release forms, required health and safety information, and pre-trip orientations and preparation. All instances of student travel to countries for which the State Department has issued a Travel Warning require USC Student Affairs and Provost approval, as specified in in SCampus.

3.14 Faculty and Staff Travel to Countries with Travel Warnings: The U.S. State Department issues periodic Travel Warnings when long-term, protracted conditions make a country dangerous or unstable. Faculty and staff who engage in foreign travel for a USC-related purpose to a country with a Travel Warning are responsible for being aware, prior to departure, of any Travel Warnings applicable to their destination country or countries. When a Travel Warning is in place, faculty and staff are responsible for enrolling in the U.S. Department of State's "Smart Traveler Enrollment Program" or "STEP" (see "Related Policies and Additional Resources"), which is a free service that provides information about current safety conditions and helps the U.S. embassy and/or family contact the traveler in an emergency.

3.15 Travel to OFAC-sanctioned Countries: Travel to an OFAC-sanctioned country (e.g., North Korea, Cuba, Syria, Iran, Sudan and the Crimea region of Ukraine as of 2016) is restricted and licensing requirements may apply to professional and research-related activities in those countries. The OFAC website provides the definitive current list of countries subject to sanction under OFAC regulation (see "Related Policies and Additional References").

3.16 Devices and Information Security: USC personnel can bring their devices containing data storage, as long as they do not contain any export-controlled technology or non-commercial, special purpose encryption software. If a device has something other than standard commercial or "mass market" encryption software, an export license may be required before taking that device overseas. International travel also poses unique information security risks compared to domestic travel. All university faculty, staff, and students should adhere to the information security practices outlined in Appendix A to protect the security and confidentiality of the information they will bring with them when they travel overseas.

3.17 Export-controlled Technology: If USC personnel intend to export items that may be export controlled (see Section 3.6 of this policy), the Office of Compliance must be contacted in all instances where the university has accepted restrictions on access or dissemination.

3.18 Biological and Chemical Materials: Taking biological or chemical samples on an international trip constitutes an export under U.S. export regulations. For example, materials that could be used for manufacture of biological or chemical weapons and chemicals that are used as propellants and high explosive materials may require specific export licenses depending on the country to which one is travelling. Also, there may be specific health and safety requirements to follow in order to safely transport these materials. USC Environmental Health and Safety should be consulted before taking biological or chemical samples abroad.

Restrictive Trade Practices and Boycotts

3.19 Participation in certain restrictive trade practices is prohibited under the EAR. Specifically, the "anti-boycott" provisions of the EAR prohibit U.S. persons or businesses from participating in any non-U.S. sanctioned foreign government boycott. As such, USC is not permitted to enter into any contract or other business relationship that requires it to participate in any non-U.S. sanctioned foreign government boycott.

4. Procedures

4.1 Sponsor demands to restrict access and/or prevent dissemination of research results: The following procedures outline how the university will address requests to conduct research where the sponsor demands the right to prevent all publication of research outcomes and/or to restrict access to research on the basis of nationality. These procedures do not apply to sponsor requirements to delay publication for a limited period of time to protect intellectual property rights or to permit review to ensure that no privileged or proprietary information has been included in a publication. Requests of this nature are permissible, as explained in more detail in Section 5-B(2) of the Faculty Handbook.

4.2 The Principal Investigator (PI) must submit a request for exception, endorsed in writing by his or her dean, to the Vice President of Research. When publication and/or personnel limitations are set forth in a proposal solicitation, exceptions must be requested in advance of proposal submission, providing sufficient time for the review process in advance of the proposal deadline. When limitations are not known until the time of award negotiation, exceptions must be requested and reviewed prior to award execution, allowing sufficient time for the review process. The request must address the following elements:

- Rationale for why the research should take place at USC
- Steps that will be taken to ensure that USC will comply with applicable personnel and/or publication restrictions
- Steps to ensure that students participating in the project, if any, will retain their rights to openly publish their own work; if this is not possible, the PI must provide assurance that no students will participate in the project
- Assurance that all project personnel (including faculty, staff, and students) have or will agree in writing to the conditions of the award

4.3 Decision on proposed exception: A decision on the proposed exception is made by the Vice President of Research upon recommendation of a standing committee of faculty from a broad range of disciplines appointed by the Provost. The Vice President of Research, or his/her faculty designee, is authorized to grant an *expedited approval without committee review* when **both** of the following conditions apply:

1. Work will be conducted in its entirety at either the Institute for Creative Technologies (ICT) or the Information Sciences Institute (ISI) and be subject to a Technology Control Plan (TCP) to ensure compliance with applicable restrictions.

2. The PI has notified the Vice President of Research about the intent to include students in the project, if applicable. Upon award of funding, Academic Affairs will initiate a process for each student participating in the project for independent (and external to ICT and ISI) academic counseling and oversight that (i) ensures that each student is made fully aware of, and agrees to, possible restrictions on publications resulting from the work on the project, and (ii) at the time the student consents to taking on restricted research (under stated publication restrictions), a plan for academic oversight is formulated that protects and outlines the student's pathway to degree completion and publications (needed for such completion). The consent needs to be in place at the time the student starts work on the project.

The Vice President of Research and/or standing committee may require that additional conditions be met, including but not limited to obtaining required licenses from the Departments of Commerce and/or State, as applicable, and implementation of a Technology Control Plan (TCP) to protect export controlled items or information. The Vice President of Research will subsequently review with the standing committee all instances where expedited approval was granted.

In the event that an expedited exception is denied by the Vice President of Research, the Principal Investigator will be given the opportunity for full committee review, at his or her request.

5. Enforcement

5.1 Under federal law, failure to comply with export control regulations (EAR, ITAR, FCPA, and/or OFAC) can result in severe fines and even imprisonment, and can be directed at both the individual and the university. For example, violations of federal law in 2016 can bring civil penalties of up to $500,000 per violation and criminal penalties of up to $1 million per violation and up to 20 years in prison.

5.2 Under USC policy, failure to comply with export control regulations and/or university-imposed requirements may also be cause for disciplinary action up to and including termination. Possible violations of this policy include, but are not limited to, engaging in an export without obtaining a license, failing to adhere to travel restrictions under OFAC, giving or receiving improper payments or other benefits to a foreign official to gain a commercial or other advantage in violation of the FCPA, and failing to adhere to university-imposed limitations on where research can take place or to the requirements of a TCP.

Sanctions for violations of this policy by a faculty member will observe all provisions of the Faculty Handbook. Sanctions for violations of this policy for staff or other non-faculty employees will observe all provisions of the staff employment policies. Sanctions for violations of this policy for students will observe all provisions contained in SCampus.

6. Definitions

6.1 "Fundamental Research": "Fundamental research" is defined as basic and applied research in science and engineering conducted at an accredited U.S. institution of higher education where the resulting information is ordinarily published and shared broadly within the scientific community. Such research can be distinguished from proprietary research, the results of which ordinarily are restricted for proprietary reasons or specific national security reasons. Research conducted by scientists, engineers or students at a university normally will be considered "fundamental research".

Information that qualifies as "fundamental research" is not subject to export control regulations. USC is committed to the widest possible public dissemination of scientific learning and research results. Therefore, the vast majority of research conducted at USC is considered to be "fundamental research" and not subject to the export control regulations.

6.2 Foreign Officials: Under the Foreign Corrupt Practices Act (FCPA), a "foreign official" includes:

- Any officer or employee of a foreign government of any rank
- Employees of government-owned or controlled businesses (including in some instances foreign university employees)
- Foreign political parties or party officials or candidates for political office
- Employees of public international organizations, such as the United Nations or World Bank

6.3 Foreign Person: Any natural person who is not a lawful permanent resident of the U. S. as defined by 8 USC Section 1101(a)(20) or who is not a protected individual as defined by USC Section 1324b(a)(3); or any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the U.S.; or international organizations, foreign governments or any agency or subdivision of foreign governments (e.g., diplomatic missions).

6.4 Business: Under the Foreign Corrupt Practices Act (FCPA), "business" or advantages may relate to, for example:

- Immigration
- Licensing
- Obtaining building permits
- Constructing facilities
- Maintaining premises in accordance with local laws
- Obtaining and maintaining work visas

- Maintaining health and safety regulations
- Routine law enforcement

6.5 Item: Commodities (including hardware), software, technology or technical services.

6.6 Technical Data: Information that is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of an Item. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. Technical data does not include basic marketing information on function or purpose or general system descriptions of Items.

6.7 Technology: Under the EAR, "technology" includes (a) specific information necessary for the development, production, or use of a product; (b) technical data including, but not limited to 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; and (c) technical assistances including, but not limited to instruction, skills training, working knowledge, and consulting services.

6.8 Technology Control Plan ("TCP"): A TCP is an internal written document that outlines the procedures that must be followed on a project-specific basis to ensure the appropriate protection of technology and/or information that is potentially subject to export control regulations, or is otherwise protected from dissemination for national security reasons.

Related Policy and Additional References

USC Faculty Handbook
Staff Employment policies
SCampus
OFAC country-specific restrictions
EAR
ITAR
FCPA
State Department Travel Warnings
State Department Smart Traveler Enrollment Program (STEP)

Responsible Offices

Office of Research
http://research.usc.edu

(213) 740-6709

Office of the Vice President for Strategic and Global Initiatives
http://global.usc.edu

(213) 740-2852

Office of Compliance
http://ooc.usc.edu

complian@usc.edu

(213) 740-8258

Executed by: **Michael Quick**
Provost and Senior Vice President, Academic Affairs

Todd R. Dickey
Senior Vice President, Administration

Date issued:

Appendix A – Information Security Measures – University-related International Travel

International travel poses unique information security risks compared to domestic travel. Adhere to the following procedures when traveling internationally to protect the security and confidentiality of information you bring with you:

1. Do not store sensitive data on any internal or external local media.
2. Leave any sensitive data stored securely on USC servers. If you need to access the data, do so via secured communications (e.g., VPN).
3. All information you send electronically by fax machine, computer, mobile phone, or other devices can be intercepted, read, deleted, and modified. Wireless devices are especially vulnerable. Avoid transmitting any sensitive data in this manner.
4. Sanitize your devices to ensure no sensitive contact, research, or personal data is on them. If feasible, use a "clean" device and a new email account while traveling.
5. Do not take information you do not need, including sensitive contact information. Consider the consequences if your information were stolen.
6. Change Wi-Fi and Bluetooth settings so they are non-discoverable and, where possible, anonymized (e.g., by resetting the default Wi-Fi MAC address).
7. Do not leave electronic devices unattended.
8. Do not use USB flash drives given to you because they may be compromised.
9. If you absolutely have to use your USB flash drive in a foreign computer, assume you have been compromised and do not use that USB flash drive again.
10. Do not open emails or attachments from unknown sources. Do not click on links in emails. Empty your "trash" and "recent" folders after every use, but be aware that information deleted from electronic devices may still be recoverable. Deleting information permanently typically requires the use of specialized software.