

## EXPORT-CONTROLLED INFORMATION OVERVIEW

This project/activity involves the use of Export-Controlled Information. As a result, the project/activity implicates either the International Traffic in Arms Regulations (ITAR) under the jurisdiction of the Department of State, or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.

It is unlawful under the ITAR to send or take Export-Controlled Information out of the U.S.; disclose, orally or visually, or transfer export-controlled information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, a license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

In general, Export-Controlled Information means activities, items, and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application utility. Export-Controlled Information does not include basic marketing information on function or purpose, general system descriptions, or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of Export-Controlled Information is military or civil in nature.

Technical information, data, materials, software, or hardware, i.e.; technology generated from this project, must be secured from use and observation by unlicensed non-U.S. citizens. Security measures will be appropriate to the classification involved. Examples of security measures are:

- **Project Personnel** - Authorized personnel must be clearly identified.
- **Laboratory "work-in-progress"** - Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
- **Marking of Export-Controlled Information** - Export-Controlled Information must be clearly identified and marked as export-controlled.
- **Work Products** - Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; preferably located in rooms with key-controlled access.
- **Equipment or Internal Components** - Such tangible items and associated operating manuals and schematic diagrams containing identified "export-controlled" technology are to be physically secured from unauthorized access.
- **Electronic communications and databases** - Appropriate measures will be taken to secure controlled electronic information. Such measures may include: User ID, password control, SSL or other approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.
- **Conversations** - Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

Each project subject to export controls must have an Technology / Export Control Plan (T/ECP) in place that outlines the procedures to be taken to handle and safeguard the Export-Controlled Information. It is the responsibility of the Project Director (PD)/Principal Investigator (PI) to develop a written T/ECP which must be approved and signed by the PI, their Department chair and Dr. Jerry Jaax, University Research Compliance Office. The PD/PI must ensure each person working on the project has read and understands this Export Controlled Information Overview and has read and understands the T/ECP. In addition, the URCO will meet with project personnel regarding the handling of Export-Controlled Information and the ECP. Project personnel must sign the Export Control Plan Certification before they can begin work on the project. Return the signed Export Control Plan and the ECP Certification to the University Research Compliance Office, Lower Mezzanine, Room 203 Fairchild Hall, Manhattan, KS 66506. Contact Information: 785-532-3224; jaax@ksu.edu. Copies of the signed T/ECP and Certification will be sent to the PD/PI, Department Chair and PreAward Services. The forms can be found on the following website: <http://www.ksu.edu/research/comply>, and at the Export/Import (EAR/ITAR) Regulations and Resources link.

## Technology / Export Control Plan (T/ECP)

This project/activity involves the use of Export-Controlled Information (ECI). As a result, the project/activity comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR) (<http://www.pmdc.state.gov>), or the Department of Commerce's Export Administration Regulations (EAR) ([http://www.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html)). Links to information about EAR and ITAR regulations are found on the University Research Compliance Office (URCO) website (<http://www.ksu.edu/research/comply>), and from the Research and Sponsored Programs Pre-awards Office, 2 Fairchild Hall.

It is unlawful under the EAR or ITAR to send or take Export-Controlled Items or information out of the U.S. This includes disclosing information orally or visually, or transferring export-controlled items or information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, an export license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

Pertinent technical information, data, materials, software, or hardware, i.e.; technology generated from this project, must be secured from use and / or observation by unlicensed non-U.S. citizens. Security measures will be appropriate to the classification involved.

In order to prevent unauthorized exportation of protected items / products, information, or technology deemed to be sensitive to National Security or economic interests, a Technology / Export Control Plan (T/ECP) may be required. If so, this is a basic template for minimum elements of a T/ECP.

## Technology / Export Control Plan (T/ECP)

In accordance with Export Control Regulations (EAR and ITAR), a Technology / Export Control Plan (T/ECP) is required in order to prevent unauthorized exportation of protected items / products, information, or technology deemed to be sensitive to national security or economic interests. This is a basic template for minimum elements of a T/ECP.

Date: [REDACTED]

Title of Sponsored Project/Activity: [REDACTED]

Technical Description of Item/Technology/Equipment/Software To Be Transferred: [REDACTED]

Responsible Individual (Project Manager / Principal Investigator (PI)): [REDACTED]

Work Address: [REDACTED]

Phone: [REDACTED]

E-mail: [REDACTED]

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

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): [REDACTED]

b. **Physical Security** (provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access, i.e. secure doors, limited access, security badges, CCTV, etc.): [REDACTED]

c. **Perimeter Security Provisions** (Describe perimeter security features of the location of the protected technology / item): [REDACTED]

2. **Information Security Plan** (Appropriate measures must 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), allowing only authorized persons to access and transmit data over the internet, using 128-bit Secure Sockets Layer (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): [REDACTED]

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

c. **Verification of Technology/Item Authorization** (describe how you are going to manage security on export controlled materials in the case of terminated employees, individuals working on new projects, etc.): [REDACTED]

d. **Conversation Security** (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. Describe your plan for protecting export controlled information in conversations): [REDACTED]

3. **Item Security**

a. **Item Marking** (Export controlled information must be clearly identified and marked as such): [REDACTED]

b. **Item Storage** (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): [REDACTED]

4. **Project Personnel** (clearly identify every person (including their national citizenship) who is determined to have authorized access to the controlled technology / item).

Name: [REDACTED]

Name: [REDACTED]

Name: [REDACTED]

**5. Personnel Screening Procedures**

a. At a minimum, you must review entities and denied parties list found on the Department of Commerce web site at <http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm>.

b. Background Checks (describe types of background checks performed on persons with access to technologies / items, i.e., criminal, drivers license, etc.):

c. Third Party Contractors (describe security screening procedures for temporary employment agencies, contractors, etc.):

**6. Training / Awareness Program**

a. Foreign Nationals (describe schedules and training for informing foreign national employees of technology access limits):

b. U.S. Employees (describe training for U.S. employees with access to controlled technology areas):

**7. Self Evaluation Program**

a. Self Evaluation Schedule (describe how often you plan to review / evaluate your T/BCP):

b. Audit Checklist (provide a checklist for items reviewed during self evaluation audits):

c. Action Item and Corrective Procedures (describe your process to address findings in your self evaluation audits):