Technology Control Plan (TCP)

This project/activity involves the use of Export-Controlled Information. As a result, the project/activity comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR) at http://pmddtc.state.gov/regulations_laws/itar_official.html , or the Department of Commerce's Export Administration Regulations (EAR) http://www.access.gpo.gov/bis/ear/ear_data.html.

It is unlawful under the EAR or ITAR to send or take Export-Controlled items or information out of the U.S. without a license or an applicable license exception. This includes disclosing information orally or visually, or transferring export-controlled items or information to a foreign person inside or outside the U.S. 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. This project has been determined ineligible for the Fundamental Research Exception/Exemption (FRE).

Pertinent technical information, data, materials, software, or hardware generated from this project must be secured from use and / or observation by unlicensed non-U.S. citizens.

Technology Control Plan (TCP)

In accordance with Export Control Regulations (EAR and ITAR), a Technology / Export Control Plan (TCP) 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 the minimum elements of a TCP.

Date: _____

Title of Sponsored Project Activity:

_____
_____
_____

Technical Description of Item/Technology/Equipment/Software to be Transferred:

_____
_____
_____
_____
_____
_____

Responsible Individual (Project Manager / Principal Investigator {PI}):

_____
_____

CSU Address: _____
Phone: _____
Email: _____

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 <u>each</u> sensitive technology / item to include building and room numbers. Attachment of a diagram of the location is highly recommended):

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

    c. **Perimeter Security Provisions** (describe perimeter security features of the location of the protected technology / item):

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:

_____
_____
_____
_____
_____
_____
_____

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 export controlled materials in the case of terminated employees, individuals working on new projects, etc.):

_____
_____
_____
_____
_____
_____
_____

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):

_____
_____
_____
_____
_____

3. Item Security

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

_____

_____
_____
_____
_____
_____

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):

_____
_____
_____
_____
_____
_____
_____

4. **Project Personnel** (clearly identify every person (including their national citizenship) who is determined to have authorized access to the controlled technology / item). Attach additional sheets if necessary. Please print.

Name & Citizenship: _____
Name & Citizenship: _____
Name & Citizenship: _____
Name & Citizenship: _____
Name & Citizenship: _____

5. **Personnel Screening Procedures**

a. At a minimum, you must review entities and denied parties lists published by the government. The Export Control Administrator will perform that review for you.

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 TCP):

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):

_____

_____

Technology Control Plan Briefing **(must be signed by all with access)**

This is to acknowledge that I have read the Technology Control Plan relating to (*insert project name or description*) and have discussed the procedures with my supervisor/PI (*name*) and I understand the procedures and agree to comply with the requirements. I agree to update this plan as required and as additional personnel are added to this project.

1) Signature: _____ Title: _____

Printed Name: _____ Date: _____

2) Signature: _____ Title: _____

Printed Name: _____ Date: _____

3) Signature: _____ Title: _____

Printed Name: _____ Date: _____

4) Signature: _____ Title: _____

Printed Name: _____ Date: _____

Original filed with ECA
Retain copy for lab/department file

CERTIFICATION ON THE HANDLING OF EXPORT-CONTROLLED INFORMATION

Overview. This project/activity involves the use of Export-Controlled Information. As a result, the project/activity comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR) at http://pmddtc.state.gov/regulations_laws/itar_official.html , or the Department of Commerce's Export Administration Regulations (EAR) http://www.access.gpo.gov/bis/ear/ear_data.html.

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 federal 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, 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.

Reasonable Care. Professors, Graduate Students, and other University individuals may be held ***personally*** liable for violations of the ITAR and the EAR. As a result, great care should be used when handling and sharing Export-Controlled Information. Individuals who will have access to Export-Controlled Information must exercise all reasonable care to follow and enforce the above Technology Control Plan. If any deviations or problems arise, the Export Control Administrator must be immediately notified. Adjusting any early deviations is much safer and preferable for all involved. By signing below, the individual primarily responsible for the Export Controlled Information certifies that they understand their responsibilities, as described in this document and the CSU Export Control Procedures Manual (ECPM), available at http://web.research.colostate.edu/OSP/export.aspx. If any questions arise, or more assistance is necessary, please contact Scot Allen, the Export Control Administrator, at scot.allen@colostate.edu.

Penalties. The penalty for the willful unlawful export and disclosure of Export-Controlled Information under the ITAR includes individual penalties of imprisonment up to 10 years and/or a fine of up to $1,000,000 per violation; penalties for the willful unlawful export and disclosure of information controlled under the EAR include individual penalties of imprisonment up to 10 years and/or a fine of up to $250,000 per violation. Similar fines are assessed to the University in the event of an individual's violation. By working with the ECA and striving for compliance, risks can be minimized for both individuals and the University.

Name of Responsible Individual _____

Department _____

Project Title _____ Project # _____

Sponsor (if applicable) _____

Certification. I hereby certify that I have read and understand this certification. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export-Controlled Information to unauthorized persons. I agree to address any questions I have regarding the designation, protection or use of Export-Controlled Information with Scot Allen, Export Control Administrator, 491-1563, scot.allen@colostate.edu.

_____ _____

Signature Date

12/13/12