General Information for Technology Control

Material, equipment, or software classified as export-controlled information under one or both of the following regulatory agencies: U.S. State Department's International Traffic in Arms Regulations (ITAR), or U.S. Department of Commerce's Export Administration Regulations (EAR) may be unlawful to disclose, orally or visually, or to transfer export-controlled information to certain foreign persons inside or outside the U.S. without an export control license. A foreign person is a person who is not a U.S. citizen or permanent resident of the U.S. The law makes no exceptions for foreign graduate students.

Therefore, depending on the type of export controlled material and the type of 'Use' contemplated, it may be necessary to restrict the use and observation of certain technical information, data, materials, software, or hardware by unlicensed non-U.S. citizens. Security measures, developed with the guidance of the Export Control Office, should be designed to be appropriate to the technology involved. Examples of security measures may include:

Physical Security:

- *Personnel Identification:* Individuals participating in the project are required to wear a badge, special card, or other similar device indicating their access to designated project areas.
- *Access logs:* Physical movement into and out of a designated project area is logged.
- *Laboratory compartmentalization:* Project operations are limited to secured laboratory areas physically shielded from access or observation by unauthorized individuals. These areas must remain locked at all times.
- *Time blocking:* Project operations are restricted to secure time blocks when unauthorized individuals cannot observe or access.
- *Locked storage:* Tangible items such as equipment, associated operating manuals, and schematic diagrams are stored in rooms with key-controlled access. Soft- and hard-copy data, lab notebooks, reports, and other research materials are stored in locked cabinets.
- *Shielding of material:* Material is physically shielded from observation by unauthorized individuals by using the material in a secured space, or during secure time blocks when observation by unauthorized persons is prevented.

Facilities

- An approved ITAR designated room is used for storage of all ITAR controlled physical materials (hardware, software, files, printed documentation).
- The ITAR room is clearly marked on the exterior door (ITAR/EAR Restricted Area – U.S. Persons only) and this approved technology control plan is posted clearly inside the room.
- The ITAR room is access controlled. The access process (room key or card) is managed by the department and all access requests are made in writing by the project PI. Only approved personnel will be granted access.
- Regular custodial, recycling and maintenance services are **NOT** to be provided in the ITAR room and facilities management is given instructions that staff are not to access the room unaccompanied. Project personnel are responsible for cleaning and/or escorting custodial -staff as visitors (as described below) for occasional cleaning and maintenance services.
- The ITAR room must have a shredder or disposal container for export controlled printed matter.

Information Security: OIT Security Office (security@colorado.edu or 303.735.6637)

- *Measures to secure controlled electronic information, e.g.:*
  - User ID, password controls, SSL or other approved encryption technology
  - Database access may be managed via a Virtual Private Network (VPN).
  - Only authorized users can access the site.

- All transmissions of data over the Internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.

- *Confidential communications:* Discussions about the export-controlled material or projects involving use of the material should be limited to authorized personnel and held only in areas where unauthorized personnel are not present.
- *Communications with third parties:* Discussions with sub-contractors and other third parties are to be avoided any and only should be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

Item Security:

- *Marking:* Export-controlled information is clearly identified and marked as export-controlled.

Personnel Security:

- *Authorized personnel:* U.S. Citizens who are authorized to use the material must be clearly identified.
- *Employee and student responsibilities:* Authorized personnel who interface with foreign nationals must receive a copy of the TCP and a briefing that addresses their export control responsibilities.
- *Supervisory responsibilities:* Supervisors of cleared personnel must ensure that employees and visitors are aware of and knowledgeable about their export controls responsibilities.
- *Training:* Export control training for all individuals associated with the project, e.g., PI, research staff, graduate students, and building maintenance is required.
- *Training certification:* Certification of training received is required.
- *Personnel additions:* New personnel must review the TCP and sign TCP certifications
- *Personnel changes:* Measures for collecting keys to project areas, removing access to project facilities, computers, and other electronic storage devices when personnel leave the project.

Technology Control Plan Template

A template is presented on the following pages.

Technology / Export Control Plan (T/ECP)

In accordance with Export Control Regulations, a Security Plan is required in order to prevent unauthorized exports 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:

Title of Sponsored Project or Activity:

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

Responsible Individual (Project Manager / Principal Investigator):

Physical Address where restricted work will be conducted:

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. A schematic of the immediate location is highly recommended.
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.
c. **Perimeter Security Provisions:** Describe perimeter security features of the location of the protected technology/item.

2. **Information Security Plan:** Appropriate measures must 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, 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 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.
e. **Graduate Thesis:** Any graduate student fulfilling their thesis research requirement with results from projects that are ITAR controlled must be a U.S. Person—or alternatively, the University must have obtained an export license for his/her participation and access to ITAR controlled technical data. In addition, the thesis advisory

committee and the participants to thesis defense must be U.S. Persons and/or an export license must have been granted for their participation and access to ITAR controlled data. Publication of the thesis and research results must be approved by the sponsor and might be delayed to meet the requirements of the research contract. Similar restrictions on access to technology/technical data apply to thesis research involving EAR controlled technology/technical data except that the restricted access by non-U.S. Persons is technology and citizenship specific.

f. **End-of-Project Measures:** After an EAR/ITAR controlled project is completed all electronic technical data/controlled information and project reports will be disposed of using appropriate wiping software. Information on "shredding" wiping software can be found at http://dban.sourceforge.net. For specific file wiping, please check Eraser, http://www.heidi.ie/eraser/default.php. and File Shredder, http://www.pcworld.com/article/231647/active_kill__hard_drive_eraser.html. Wiping an entire device is the preferred solution.

g. **Departure from the University:** The procedures outline above for electronic data disposal will be used with a PI of an EAR/ITAR controlled project is departing from the university.

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" technologies are to be physically secured from unauthorized access.

4. **Project Personnel** clearly identify every person, who is determined to have authorized access to the controlled technology/item.

a. Name:	**Country of Citizenship:**
b. Name:	**Country of Citizenship:**
c. Name:	**Country of Citizenship:**

It is the responsibility of the Principle Investigator to inform the Export Controls Office of any new addition to the project personnel. You may contact the Export Controls Office at: exportcontrol@colorado.edu or Phone: 303 492-2889. The TCP will be updated accordingly.