

**Arkansas State University – Jonesboro**  
**Technology Control Plan**  
**Department Approval**

A Technology Control Plan (TCP) is required for research which deals with technical items, data, and/or software controlled by U.S. Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR). The requirement applies to all research activities whether or not they are externally sponsored. The TCP should specifically address the following:

- A) Personal Training – Awareness and basic understanding of export restrictions; document time and date of training. **NOTE:** All laboratory personnel should receive basic training.
- B) Personnel Screening – Identify of foreign nationals with physical access to the laboratory area; identity, residency status, and project role of ASU-Jonesboro participants; identity of person with primary responsibility for security of controlled items/materials/equipment (usually the Principal Investigator but may be a senior member of the research team).
- C) Physical Security – Laboratory and building access escort requirements, visitor logs, etc.
- D) Equipment Access – Identification of controlled laboratory equipment and methods for restricting access
- E) Information Security – Control of access to both electronic and physical data and information, software, and prototype.
- F) Internal security evaluation – Periodic review and audit of internal controls to identify and report findings of any unauthorized export.
- G) Statement that participants are not on any of the following lists:
  - a. Denied Persons List
  - b. Unverified List
  - c. Entity List
  - d. Specially Designated Nationals List
  - e. Debarred List
- H) Statement that a) controlled items have been or will be identified for all participants prior to access; b) all participants having access to controlled items have been informed of the security measures to be used in controlling access; c) participants will be adequately supervised by the person responsible for access control to prevent the export to unauthorized persons.
- I) Signature of the Foreign National in which this plan is executed and acknowledges its existence.
- J) Signature of Principal Investigator and, if different, the person with primary responsibility for access control.
- K) Signature of Department Head/Chair or unit equivalent acknowledging approval to engage in controlled research activities as described.

## Technology Control Plan

### Department Approval

Principal Investigator \_\_\_\_\_

Phone: \_\_\_\_\_ Email: \_\_\_\_\_

Campus Address: \_\_\_\_\_

Foreign National Name \_\_\_\_\_

Country of Origin \_\_\_\_\_

Locations Covered by Plan (Buildings and Rooms):

---

---

Sponsors, if applicable \_\_\_\_\_

| Funding Agency | ASU Fund<br>Number | Project Period |     | Contractual<br>Obligations or<br>Restrictions | Non-Disclosure<br>Agreements |
|----------------|--------------------|----------------|-----|-----------------------------------------------|------------------------------|
|                |                    | Start          | End | (Yes/No)                                      | (Yes/No)                     |
| _____          |                    |                |     |                                               |                              |
| _____          |                    |                |     |                                               |                              |
| _____          |                    |                |     |                                               |                              |

List contractual obligations, restrictions and all parties to any non-disclosure agreements:

---

### Attachments:

Describe in detail the following steps taken to prevent the release of controlled items/information.

- |                                     |                         |
|-------------------------------------|-------------------------|
| A. Personnel Screening and Training | D. Physical Security    |
| B. Physical Access                  | E. Information Security |
| C. Internal Security Evaluation     |                         |

## Certification:

By signing below, I certify I am committed to the protection of controlled items in accordance with U.S. Export Administration Regulations and that the statements contained herein are accurate and truthful to the best of my knowledge. I further certify that a) controlled items/materials/data/ equipment have been or will be identified for all participants prior to allowing access; b) all participants having access to these controlled items will receive basic training in U.S. Export Administration Regulations and be informed of the security measures to be used in controlling access to project information prior to access; and c) all participants will be adequately supervised by me, the Principal Investigator, or by the person designated the primary responsibility for access control if other than myself.

I have contacted the Office of Research Compliance to verify that no personnel working on this project are on any of the following Lists: 1) Denied Persons, 2) Unverified, 3) Entity, 4) Specially Designated Nationals, and 5) Debarred/Suspended.

PRINTED NAME

SIGNATURE

DATE

---

Foreign National

---

Principal Investigator

---

Designated Control Person (other than PI)

---

Department Head/Supervisor

## TECHNOLOGY CONTROL PLAN

### Laboratory Personnel

Prepared By (PI) \_\_\_\_\_ Date: \_\_\_\_\_

Title and Affiliation: \_\_\_\_\_

Contact Information: Phone: \_\_\_\_\_ Email: \_\_\_\_\_

Address: \_\_\_\_\_

Foreign National Name: \_\_\_\_\_

Country of Origin/Citizenship: \_\_\_\_\_

Laboratory Location: \_\_\_\_\_

#### 1. Research Projects and Controlled Information:

Current research and personnel in the \_\_\_\_\_ laboratory are sponsored by \_\_\_\_\_ different sources:

- a.
- b.
- c.

Results from the research in the \_\_\_\_\_ laboratory will be presented at scientific conferences (poster and oral presentations) and invited talks within the US and abroad or publications in peer-reviewed journals or book chapters.

If inventions with economic impact could be derived from any of these research projects in the \_\_\_\_\_ Laboratory or through a collaborative initiative with another institutions or companies, then it will be submitted as utility patent application before any disclosures are made in the US or abroad.

#### 2. Controlled Laboratory Equipment and Instrumentation

Items below have been discussed with the Arkansas State University Director of Research Compliance and they represent controlled equipment, software, or instrumentation. Every item mentioned below has a sign-in sheet to log in date and time in which the equipment or instrument is used. First access to a controlled equipment or instrument requires authorization by \_\_\_\_\_. Access to the equipment assembly manuals and software will be restricted and secured in a locked cabinet.

All controlled equipment will be identified to all current and new personnel by \_\_\_\_\_ in the \_\_\_\_\_ Laboratory and they will be informed of the security measures to be used in controlling access. The controlled items including manufacturer and their locations include:

| DESCRIPTION | BRAND | MODEL | SERIAL NUMBER |
|-------------|-------|-------|---------------|
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |
|             |       |       |               |

### 3. Data Security

All members of the \_\_\_\_\_ laboratory will sign a non-disclosure agreement on the first day of work and this signed form is required before attending any meetings with \_\_\_\_\_. (If it relates to your laboratory.)

Any data from experiments in the laboratory will be sent electronically using the secure network connection of Arkansas State University. External hard drives will be used to back-up information and these external drives will be under the controlled of \_\_\_\_\_. All computers in the \_\_\_\_\_ laboratory containing research and analytical data will be password protected and these passwords will be only available to authorized users.

### 4. Personnel in the \_\_\_\_\_ laboratory with authorized access to controlled equipment or information include:

| PERSONNEL                     | CITIZENSHIP | VISA STATUS |
|-------------------------------|-------------|-------------|
| Principal Investigator --     |             |             |
| Other Laboratory Personnel -- |             |             |
|                               |             |             |
|                               |             |             |
|                               |             |             |
|                               |             |             |
|                               |             |             |
|                               |             |             |

### 5. Personnel Screening Procedures

The Arkansas State University Director for Research Compliance will be in charge to check if any laboratory personnel are in the following lists by using the Visual Compliance Software:

- Denied Person List
- Unverified List
- Entity List
- Specially Designated Nationals List

e. Debarred List

6. Training and Awareness Program

All members in the laboratory are required to take the CITI training on Export Controls. Completion reports and a spreadsheet with the dates of completion will be kept by \_\_\_\_\_ and a copy of the reports will be housed with the Director of Research Compliance. All personnel in the \_\_\_\_\_ laboratory will receive all safety and compliance training mandated by the Arkansas State University- Jonesboro. In addition, the laboratory personnel also receive specific training concerning research areas of the laboratory. Training and awareness of the Technology Control Plan will be included in this initial training and the time and date of training will be recorded.

7. Self-Evaluation Program

The Technology Control Plan will be evaluated every 4 months. During the evaluation log sheets for all the controlled equipment/instrumentation will be reviewed and special attention will be given to foreign nationals (non-permanent US residents) that have used this equipment/instrumentation. A check for any new equipment/instrumentation that needs to be added to this controlled equipment/instrumentation list will be done. Passwords to selected computers will be checked and changed. We will make sure that all critical data have been backed-up. Action items and corrective procedures will be implemented upon reviewing the first evaluation. For instance more frequent unscheduled checks will be included to closely monitor any controlled item in the laboratory.

**Review and Approval by University Authorized Official:**

---

Name:

(Required for all Project Personnel identified in the Technology Control Plan)

**Reasonable Care:** You may be held personally liable for violations of the ITAR or EAR. As a result you exercise care in using and sharing Export-Controlled Information/Technology with others. Controlled Information/Technology must be handled in accordance to the security plans and/or controls specified in the Technology Control Plan and only shared with authorized Project Personnel. In the absence of that clearance, PIs or designated controls individuals should not leave Export-Controlled information/Technology unattended.

**Certification:** I certify I have read, understood and will adhere to this Technology Control Plan as it is applicable to the EAR and ITAR regulations.

DATE \_\_\_\_\_

[illegible]