UNIVERSITY OF NOTRE DAME | RESEARCH Administration

Technology Control Plan

TCP Reference Number:

RESPONSIBLE OFFICE CONTACT:

Notre Dame Research Administration
940 Grace Hall, Notre Dame, IN 46556
Phone: (574) 631-7432
Fax: (574) 631-6630
E-mail: rca@nd.edu

In the event of any suspected breech of physical or electronic data should be reported immediately to the NDRA Export Control Officer.

Section A- General Project Information (section to be completed by Export Control Office (ECO)

1. Project Title: **Working/Reference Title (If applicable):**		**2. Sponsor (& Prime Sponsor, if applicable):**	
3. Project Period:	**Start date:** **End date:**	**4. Export Control Jurisdiction** (select one)	Multiple
5. Principal Investigator (PI):		**6. Technology Control Plan Type** (select one)	Software Only
7. PI Email & Phone number:		**8. ECO Preparer:**	
9. Sponsor Contract Number:		**10. Grant Number:**	

11. Acknowledgment and Acceptance of Principal Investigator (PI):
I understand my responsibilities as a PI on this export controlled project. I have read the Technology Control Plan and have discussed the plan with the NDRA Export Control Officer. I understand the plan and agree to comply with all its requirements. I affirm that the project personnel, advisory committees, dissemination of controlled information will fit within the parameters of the referenced ECCN/ ITAR categories to prevent unauthorized or unlicensed exports, re-exports, or deemed exports. I agree to participate in regular audits and enhancements to this TCP. I will ensure that project personnel are briefed of their responsibilities under this Technology Control Plan and have signed in acknowledge before being granted access to controlled information, material or equipment. I understand that diversion contrary to the approved plan is prohibited. During the conduct of the project, if any question arises as to the implementation of the measures herein, I will seek clarification from the NDRA Export Control Office.

Signature:	**Date:**
Individual authorized to speak on PI's behalf for issues related to this TCP (complete only if applicable)	

12. Acknowledgment of Information Security:
This Technology Control Plan has been reviewed by a technically-capable IT Security person from Information Security to ensure that regulatory and IT security requirements (as identified in Section E. herein) can be implemented and that apparent security concerns have been addressed.

Information Security: **Jason Williams**	**Signature:**	**Date:**

13. Acknowledgment of Lead Department Head:
I acknowledge that this project will be conducted in my department and I understand that the controls listed within this Technology Control Plan are required by federal regulation and university policy. If I become aware of a breach or violation of this Technology Control Plan, I will inform the Export Control Officer immediately.

Department:	**Name:**	**Signature**	**Date:**

14. Accepted by Export Control Officer:

Name: **Greg Luttrell**	**Signature:**	**Date:**

The answers and information listed within this plan should be accurate and complete as of the time the plan is put in place. In the event of the any of the following actions, please contact the ECO to file an amendment to the plan.

- **Significant changes to the scope or project plan (including any new effort not originally proposed)**
- **Personnel additions or deletions**
- **IT hardware additions or deletions**
- **IT storage or software changes**
- **Physical location (office or lab additions or change)**
- **Significant changes to the physical security**
- **Change to Student thesis/dissertation committee or new plan of study submission.**

Export Control Guidelines can be found at https://research.nd.edu/assets/187714/export_control_guidelines.pdf

Section B – Summary of Project and Control Requirements

1. Provide a brief description of the project.

2. Reason for Technology Control Plan: (i.e. access, publication restriction, etc.) (To Be completed by ECO)

3. ECCN/USML Category (list the Export Control Classification Number and paragraph or ITAR Category and paragraph) **(To Be completed by ECO)**

4. Summary of Citizenship Restrictions. (To Be completed by ECO)

5. Do Non-U.S. Persons need to be approved by Sponsor? (To Be completed by ECO)	○	Yes	◉	No

6. What type information, material and/or equipment will need to be protected by the controls set forth in this TCP (Select all that apply)		
	☐	**a) Technical Data received from an External Source (Sponsor, collaborator, etc.)**
	☐	**b) Technical Data generated by my research team**
	☐	**c) Equipment/Software** **description:**
	☐	**d) Materials (e.g. energetic materials, fuel, carbon nanotubes, etc.)** **description:**
	☐	**e) Items that will leave the U.S.**
	☐	**f) Other** **explain:**

7. If additional forms or plan addendums are needed to complete this TCP (e.g. Personnel, student Thesis, IT, Co-PI collaborative plan), please list below. (to be completed by ECO)

Section C - Personnel

1. Clearly identify every person (including their citizenship/permanent residency), who will require authorized access to the controlled technology / item using the table below. Access to controlled information should be limited to only those individuals who have a legitimate need to know, have been briefed on the specifics of this plan, and have signed in acknowledgment below. Note - You may attach an Additional form – Personnel, as needed.

* PI should ask citizenship/permanent residency question of each individual. The ECO will attempt to verify through HR. If they cannot, an individual may be asked to provide citizenship document before being granted access to controlled information.

Project Personnel Acknowledgment: **My signature below is confirmation that I have been briefed of my responsibilities related to controlled information and technology under this project and will adhere to the controls outlined. If I become aware of a breach or issue, I will report it immediately to the PI and/or the Export Control Office contact listed on the front of this plan.

Full Name	DEPT	Role on Project (student, postdoc, etc.)	Country of Citizenship (or permanent residency)*	Advisor (for student/ postdocs) or Supervisor	Date of Training Completed (completed by ECO)	Signature**
						See first page for signature

If there are Co-Investigators in departments different than the primary department listed on page 1:

2. Acknowledgment of co-PI Department Head(s):

I acknowledge that elements of this project will be conducted in my department and I understand that the controls listed within this Technology Control Plan are required by federal regulation and university policy. **If I become aware of a breach or violation of this Technology Control Plan, I will inform the Export Control Officer immediately.**

a. Department:	**Name:**	**Signature**	**Date:**
b. Department:	**Name:**	**Signature**	**Date:**
c. Department:	**Name:**	**Signature**	**Date:**

Section D - Physical Security	
1. Building Location of Controlled Information/Project:	**2. Who is the Facility Manager? (Name and email)**
3. Describe the physical location of each sensitive technology/item/research activity. Include building and room numbers. Reference to a diagram or picture (attach if needed) of the immediate location is highly recommended.	
4. Provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access. Make sure to include a detailed description of secure doors, locked cabinets, and limited access. If there are Foreign Persons (students, faculty, staff and/or visitors) in close proximity to this controlled space, please include steps you take to address that additional factor. A Foreign Person, by Export Control regulations, means a person who is not a U.S. citizen or lawful permanent resident.	
5. Describe your plan for protecting export controlled information in conversations (e.g. Informal conversations and more formal discussions like lab meetings, presentations, etc.)	

Section E - Information Technology Security

1. Are there NIST or contract-based standards on IT? (To Be completed by ECO)	○	Yes	○	No

2. Describe the location of each computer/workstation that will access export-controlled information. Note - You may attach an Additional Form – IT, as needed.

	Type of Information System (IS)	Location	Device and unique ID (e.g. Dell Laptop & SN, or AWS GovCloud Instance #, removable or portable media & SN)	Managed by (e.g. ESC, CRC, or locally managed)*	Will it Store Controlled Information?	Encryption? 128-bit or higher)	Connected To a printer?
a.	Portable Device				No	No	Yes - Network
b.	Portable Device				No	No	Yes - Network
c.	Portable Device				No	No	Yes - Network
d.	Portable Device				No	No	Yes - Network
e.	Portable Device				No	No	Yes - Network
f.	Portable Device				No	No	Yes - Network
g.	Portable Device				No	No	Yes - Network

3. If an IS listed above is locally managed, Please indicate how antivirus updates and patches are provided and who does repair and maintenance. Note, while devices can be locally managed, they must be **owned by University of Notre Dame**. In some cases, sponsored provided IS may be used, when approved by the ECO. **No personally owned devices can be used to access or store controlled information.**

4. If any IS listed above is a portable device, describe access and controls for the physical security of these items. For the purpose of this question, laptops should be considered portable devices.

5. For physical systems, describe the measures in place to prevent unauthorized viewing of these machines when processing controlled information (screen savers, privacy filters, screen placement, etc.)

6. For items listed above, if encryption is indicated, please list the plan for encryption. (e.g. Bitlocker)

7. Who is your primary IT contact in the event of a computer problem? (Please provide contact information.)

8. If controlled Information will be shared (sent or received) electronically, describe the secure method that will be used. (Via encrypted e-mail, CD, sponsor provided secure file sharing system, etc.).