Technology Control Plan

I. Statement of policy and assignment of responsibility

The University of Illinois at Urbana-Champaign (UIUC) is committed to complying with the export laws and regulations of the United States. This commitment is described fully in Campus Administrative Manual policy XI-3, available at http://cam.illinois.edu/xi/xi-3.htm. The Responsible Employee identified below has the primary responsibility for complying with these laws, regulations, and policies with respect to the Controlled Items identified below. This technology control plan (TCP) contains the specific measures that the Responsible Employee and other identified personnel will take to protect the Controlled Items from improper access or disclosure.

II. Administrative information

Responsible Employee:

Phone number: Email:

Unit/Department: Unit Head:

III. Controlled Items

The Export Compliance Officer (ECO) has determined that the following items and/or information (referred to in this TCP as Controlled Items); as such, access to and disclosure of these Controlled Items to foreign nationals requires a valid export license or other governmental authorization. For this reason, only the Responsible Employee and the other Authorized Personnel identified in Attachment A of this TCP may access the Controlled Items covered by this TCP. The ECO will work with the Responsible Employee to obtain any required export licenses or other authorizations.

The Controlled Items covered by this TCP are as follows:

	Description[1]	Type	Jurisdiction	Classification[2]
1		Select one...	Select one...	
2		Select one...	Select one...	
3		Select one...	Select one...	
4		Select one...	Select one...	
5[3]		Select one...	Select one...	

[1] Wherever possible, please provide the manufacturer and model.
[2] Provide the applicable United States Munitions List category and subcategory for any Controlled Items subject to the ITAR, or the Export Control Classification Number (ECCN) if subject to the EAR.
[3] If there are more than 5 Controlled Items, additional space is provided in Attachment B.

IV. Security strategy

A security plan should explain how you plan to protect the Controlled Items listed in this TCP against loss, theft, and unauthorized visual inspection. A comprehensive plan will address physical and information security in terms of storage, use, and transmission.

a. Physical security

Location(s)

Controlled Items may only be used and stored in secure locations. Secure locations have defined perimeters that allow for protection against inadvertent disclosure of Controlled Items. Consider spaces that have physical barriers like walls that would prevent unauthorized individuals from seeing or overhearing discussions involving Controlled Items. Only the Authorized Personnel identified in Attachment A will be allowed to enter the secure locations while Controlled Items are in use. In most circumstances, a secure location can be used for other purposes, or by other people, whenever the Controlled Items are securely stored and not in use. Please note any locations that will be used for other purposes in addition to hosting Controlled Items.

Identify the location(s) where you will store and/or use the Controlled Items:	

Storage

Controlled Items, including physical equipment, materials, and hardcopy data, must be secured in a locked room or other locked, opaque containers when not in the personal possession of Authorized Personnel. Electronic devices, like computers and mobile devices, that contain sensitive information must also be physically secured when not in the possession of Authorized Personnel. Keys and lock combinations may only be shared with Authorized Personnel. Consider the size and sensitivity of the Controlled Items and note any special arrangements you will need to make. **Note that electronic information security is addressed in a separate section and should not be described here.**

Identify the methods you will use to physically secure the Controlled Items when they are not in use:	

Markings

Whenever possible, Controlled Items should be clearly marked with an appropriate warning. For example:

> **WARNING: This item/document contains technical data subject to export controls. Unauthorized access may result in prosecution and severe criminal**

penalties. Contact the Export Compliance Officer (300-6385 or exportcontrols@illinois.edu) if you find this item/document unsecured.

If physical space is limited, you may use an abbreviated warning. For hardcopy or electronic documents, you may also use headers, footers, or watermarks.

b. Information security

Computers and electronic devices

All computers and servers used to access or store Controlled Items must run on Microsoft Windows 7 or later, Mac OS X or later, or other operating systems offering comparable security features. Operating systems must be kept up to date with the latest service packs, security patches, and virus/malware protection. Only Authorized Personnel may be designated users of computers and servers used to access or store Controlled Items. Access permissions must be managed through Active Directory or other service offering comparable security features and the ability to log both successful and failed login attempts. Firewalls must be installed to monitor inbound and outbound network activity. **Note that access to these computers and servers must be limited to US nationals, including for technical support. DO NOT use personal computers to access or store ITAR-controlled information.**

List all IT resources (computers, servers, etc.) that will be used to access or store controlled information, including controlled software:	
Describe the steps you will take to secure these IT resources:	

Data storage and transmission

Whenever possible, you should use external hard drives, flash drives, or other physical media for storing Controlled Items when not in use. Drives and devices used to store Controlled Items must be password-protected and encrypted (whole disk, using PGP, AES-128, or comparable algorithms). For data storage on drives with network access or backup servers, files and folders containing Controlled Items must be password-protected and encrypted. **DO NOT upload Controlled Items to cloud services.**

When transferring electronic Controlled Items, you must use a secure file transfer method (like SSH/SFTP or encrypted email) or send physical media via post. **DO NOT use unsecured email domains (Yahoo!, Gmail, etc.) to transfer Controlled Items.**

Describe your plan for storing controlled data and any methods you will use for transmitting controlled data:	

V. Exports and international travel

Explain any intended exports of Controlled Items. Include the item to be exported, the intended recipient, the recipient's location as specifically as possible, the recipient's intended use of the Controlled Item, and whether the Controlled Item will be returned to you.

Exports include shipping or carrying Controlled Items out of the United States (including for your own use while abroad); accessing a Controlled Item from outside the United States; disclosing (including permitting visual inspection) or transferring a Controlled Item to a foreign national[4] inside the United States; or disclosing a Controlled Item (including permitting visual inspection) to anyone outside the United States, regardless of nationality.

Note that including a planned export here DOES NOT constitute authorization to carry out the export; a license or other authorization may still be required. Only the Export Compliance Officer may apply for any required licenses or authorizations on your behalf.

Explain any planned exports of Controlled Items:	

In particular, if you plan to travel to an embargoed country[5] for any reason, including personal travel, you must notify the Export Compliance Officer at least sixty (60) days prior to departure.

VI. Disposition of Controlled Items

Upon completion of the relevant projects, the Controlled Items must be disposed of in accordance with applicable sponsor terms, federal export control requirements, and Illinois state law. The Responsible Employee must contact the Export Compliance Officer at project completion to coordinate the disposition or maintenance of Controlled Items beyond the life of any relevant project(s).

[4] A foreign national is anyone who is not a United States citizen, permanent resident, or protected individual.
[5] Embargoed countries include: Cuba; Iran; North Korea; Sudan (aka North Sudan or the Republic of Sudan); and Syria.

VII. Other notes

Explain any other terms or circumstances that should be considered for this TCP:	

VIII. Authorized Personnel requirements

a. Identification

All Authorized Personnel who require access to the Controlled Items must be identified in Attachment A and sign a TCP Acknowledgement (form EC-002). The Responsible Employee may request the addition or removal of Authorized Personnel at any time by sending a written request to the Export Compliance Officer (exportcontrols@illinois.edu).

b. Training

All Authorized Personnel must satisfactorily complete an export compliance training program prior to accessing any Controlled Item. Training consists of an overview of federal export control regulations, an explanation of the responsibilities imposed by this TCP, and a notification of the potential criminal and civil penalties (including prison sentences of up to 20 years and fines of up to $1,000,000 per violation) for failure to comply with US export controls. Training sessions can be scheduled on an individual or group basis by contacting the Export Compliance Officer (exportcontrols@illinois.edu).

c. Screening

The Export Compliance Officer will screen proposed Authorized Personnel against the applicable lists of restricted parties to determine licensing requirements based on country(ies) of citizenship or permanent residence. The Responsible Employee will not allow individual personnel to access the Controlled Items until the individual has signed a TCP Acknowledgement, completed the required training, and been authorized by the Export Compliance Officer. Foreign nationals will only be authorized to access the Controlled Items after all license requirements have been fulfilled by the issuance of a valid export license or documentation of an applicable license exemption.

IX. Associated agreements

In order to ensure compliance with sponsor terms regarding the use and disposition of the Controlled Items, please list any associated agreements, including funded or unfunded research agreements, purchase contracts, etc.:

	Title or description	Sponsor/vendor/etc.	Agreement number	Agreement type
1				
2				
3				
4				
5				

X. Internal notification and assessment

a. Notification

The Responsible Employee will notify the Export Compliance Officer in the following circumstances:

1. Prior to adding new personnel;
2. When the scope of the use of the Controlled Items changes;
3. When there is a change in funding or in award terms or conditions; and
4. To request any other modification to the TCP, including adding or removing Controlled Items.

b. Assessment

The Responsible Employee and Department agree to cooperate fully with any compliance assessments initiated by the Export Compliance Officer. Compliance assessments may be conducted as in conjunction with the annual renewal of this TCP, for cause, or as part of a random assessment process.

c. Period of validity

This TCP is valid for 12 months beginning on the date of acceptance by the Export Compliance Officer. This TCP may be renewed every 12 months upon satisfactory completion of a compliance assessment conducted jointly by the Export Compliance Officer, the Responsible Employee, and the Department.

XI. Acknowledgements

Responsible Employee:	_____	_____	_____
	Printed name	Signature	Date
Department head:	_____	_____	_____
	Printed name	Signature	Date
Export Compliance Officer:	_____	_____	_____
	Printed name	Signature	Date

Assigned TCP number:

Attachment A (required)

Authorized Personnel

	Name	U of I email	Immigration status	Country of citizenship
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

TCP number: TCP-_____

Attachment B (optional)

Additional Controlled Items

	Description[6]	Type	Jurisdiction	Classification[7]
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

[6] Wherever possible, please provide the manufacturer and model.
[7] Provide the applicable United States Munitions List category and subcategory for any Controlled Items subject to the ITAR, or the Export Control Classification Number (ECCN) if subject to the EAR.

Appendix

UIUC has an obligations to report foreign government talent recruitment program interactions While the U.S. Department of Energy (DOE) encourages international collaborations at the national laboratories, all federal agencies have growing concerns about the national and economic security risks associated with international research and collaborations involving sensitive foreign countries. The intent is not to stop international collaborations, but to protect specific science and technology. To address these concerns, on June 7, 2019, DOE issued an order, establishing new requirements for reporting talent recruitment programs operated or funded by foreign countries. (The definition of a Foreign Government Talent Recruiting Program is included in the Order.)

Association with talent recruitment program by itself is not illegal; however, potential participants and their employers should be aware of legal issues that may arise as a result of participation, including violation of export-control laws, economic espionage, or violation of employer conflict-of-interest policies.

Please identity any foreign affiliated sources of funding or membership in a Foreign Government Talent Recruitment Program for members included in this project.

Description	Type