Technology Control Plan

Statement of Institutional Commitment

The University of Virginia is committed to complying with applicable export control, embargo and trade sanction laws and regulations in all university activities. This commitment is articulated in University policy FIN-043 *Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of Research and Scholarship* and the associated Export Control Management Program. This Technology Control Plan (TCP) identifies the specific measures that will be taken by Responsible Person, a UVA executive or faculty member unless prior approval is obtained from the Office of Export Controls (OEC), and all project personnel to ensure compliance with those requirements.

Responsible Person _____ Department _____

Covered Items and Information

The following items or information have been determined to be subject to export control requirements which require that the University place limitations on who may have access to or use the items or information, hereinafter called *Covered Items and Information*. A variety of factors must be taken into account to determine who may have access to *Covered Items and Information*; for this reason, only individuals who are identified below and have been approved by the Office of Export Controls may have access.

A list of the *Covered Items and Information* that will be protected under this TCP is provided in the table below:

#	Name or Description	Type	Jurisdiction	Classification*
1		Select One	Select One	
2		Select One	Select One	
3		Select One	Select One	
4		Select One	Select One	
5		Select One	Select One	
6		Select One	Select One	
7		Select One	Select One	
8		Select One	Select One	

** Provide the applicable US Munitions List category and subparagraph if subject to the ITAR, the Export Control Classification Number (ECCN) if subject to the EAR, or the paragraph and subparagraph if subject to the DoE nuclear regulations.*

Note: If more than eight entries are needed, additional space is provided on the last page of this document.

As a result of this determination, the Responsible Person, identified above, has worked with OEC to develop this TCP to ensure that *Covered Items and Information* are adequately protected from disclosure to foreign persons without an approved license, valid license exception, or other written government approval.

Security Overview

"One Lock" is the principal of securing items and information by using at least one mechanism to prevent access by unauthorized persons. This is the minimum requirement for safeguarding the *Covered Items and Information*, listed above. Methods for obtaining at least "one lock" are described in the physical and information security sections below. Project personnel are responsible for safeguarding *Covered Items and Information* at all times by having "one lock"; this includes preventing visual access if such access could provide technical information about an item.

Physical Security

Work Area. Locations where work is to be performed with *Covered Items and Information* shall have restricted access. Restricted access is defined as having a clearly defined perimeter, which is adequate to protect against oral, in the case of discussions involving *Covered Information*, and visual disclosure of the *Covered Items or Information*. Physical barriers are strongly recommended but are not required as long as oral and visual disclosure can be prevented. Project personnel within the Restricted Area shall be responsible for challenging all persons who may lack appropriate access authority.

Specify the location(s) where work will be performed with the covered items and information.	

Storage. All export *Covered Items and Information* (hard copies) will be secured in a locked room, storage device or container when not in the personal possession of approved project personnel. Keys or combinations to storage containers used to secure *Covered Items and Information* will only be issued to the approved project personnel authorized on this TCP. Electronic devices containing *Covered Items and Information* must be physically secured or in the possession of an approved user at all times. *Note: Security of electronic files should be addressed in the Information Security section, below, rather than here.*

Specify the location(s) where the covered items and information (hard copies) will be stored when not is use.	

Marking. Whenever possible *Covered Items and Information* should be clearly marked with an appropriate warning, for example: *WARNING - This contains ITAR controlled technical data. Access or dissemination in violation of the ITAR may result in severe administrative (institutional) and criminal (individual) penalties. Contact the UVA Office of Export Controls (x2-5725 or export-controls@virginia.edu) if you find this item/document unsecured.* When physical space is limited, an abbreviated warning may be used, for example: *Export Controlled - ITAR*. Watermarks, headers or footers may be used to mark electronic documents.

Describe the markings or warnings that will be placed on covered items and information or explain why they are not practical or possible.	

Information Security

Computer. All computers used to access or store *Covered Items and Information* must run Microsoft Windows XP, Windows 7, Vista, Mac OS X, or Linux with the latest security service pack and patches; similar requirements apply to servers and other devices. Generally speaking only approved project personnel should be designated users of computers and servers used to access or store *Covered Items and Information* and a valid account and password must be provided to gain access. Only approved project personnel retain this login information and no other login accounts are created. Both failed and successful logins are logged internally. Firewalls are installed on all computers to secure and monitor network access to/from the computer. If the firewall must be disabled to allow proper data collection, wired and wireless internet connections must be disabled. *Note: Administrative access by central, school or departmental IT personnel must be limited to US persons (citizens, permanent residents or protected individuals).*

List all IT resources (computers, servers, systems, etc.) that will be used to store or process Covered Items and Information.	
List all individuals with administrative access to IT resources who are <u>not</u> Project Personnel.	
Describe any project specific security methods, devices or procedures that will be employed to assure computer security.	

<u>Data Storage and Transmission</u>. External portable hard drives or flash drives, rather than shared central servers, are recommended for data storage provided physical storage is employed when they are not in use. Drives and devices used to store *Covered Items and Information* must be password protected or encrypted. For data storage on drives with network access or backup servers, the *Covered Items and Information* must be secured by encryption and password protection. Email may not be used for the transfer of *Covered Items or Information* subject to the ITAR or EAR. A secure file transfer method (SSH/SCP/SFTP/SSL) or mailing a disk or flash drive are preferred methods to transfer *Covered Items and Information* in electronic format. *Note: Emailing Covered Items or Information subject to control regimes other than the EAR and ITAR will be considered on a case-by-case basis, but is <u>not</u> authorized unless specified below; when authorized to use email, the sender's is responsible for ensuring that the recipient is physically present in the US at the time of transfer.*

Describe any project specific security methods or procedures that will be employed for data storage and transmission.	

<u>Supercomputing and Cloud Computing</u>. Unless specified below no supercomputing or cloud computing facilities or services will be used to store, process or transfer *Covered Items or Information*.

Describe any intended use of supercomputing or cloud computing facilities or services.	

Export Control Risks

<u>Award Terms.</u> When the terms of an award contain explicit export control requirements; foreign national restrictions; or require that the sponsor's approval be obtained prior to publication or dissemination of research results, UVA will typically treat the project as subject to US export controls. In such cases, the research results must be identified as *Covered Items and Information*, above.

Export Control Risks (cont.)

Nondisclosure/Confidentiality. In most cases, proprietary information provided to UVA under confidentiality conditions will be presumed to be subject to US export controls and may not be shared with foreign nationals without the approval of OEC.

Student Involvement. Student participation on projects that require the sponsor's permission to publish or where results are subject to US export controls must be limited to work which is not required for the completion of their degree or program without the explicit approval of the student's Department Chair, Dean's Office and the Office of the Vice President for Research. Students may have access to background proprietary information only to the extent permitted by the applicable export control regulations.

Project Specific Export Authorizations

Specify any intended exports of *Covered Items and Information* in the section below. Inclusion in this section does NOT, in and of itself, constitute approval to export; it is rather an indication to OEC that an export license or other authorization may be needed. This prohibition on exports includes, but is not limited to, exports to foreign nationals in the US, as well as the permanent or temporary shipment or transfer of *Covered Items and Information* out of the US.

Specify any planned exports of *Covered Items and Information*.	

Special Notes

Use the space below to provide any project specific notes or clarifications.

List any other project specific requirements or conditions in the space provided.	

Project Personnel Requirements

Identification: All project personnel needing access to *Covered Items and Information* must be identified in *Appendix 1: Personnel List* and sign an *Acknowledgement of Responsibilities*. The Responsible Person may request the addition or removal of project personnel at any time by submitting a *Revised TCP* to the OEC (export-controls@virginia.edu).

Training. All project personnel are required to complete the University's export control training program prior to having access to *Covered Items and Information* or participating in any export controlled aspect of this project. Annual refresher training is required for all project personnel. As part of training, project personnel are made aware of what constitutes an export, their responsibilities to prevent both active and inadvertent disclosures of *Covered Items and Information*, and of the criminal and civil penalties (including prison sentences of up to 10 years and fines of up to $1M per violation) for failure to comply with US export control laws.

Screening. The OEC will screen all project personnel against the applicable lists of restricted parties and will determine licensing requirements based on their country(ies) of citizenship, nationality, or permanent residence. The Responsible Person shall not allow project personnel access to *Covered Items and Information* until the individual has signed *Attachment A*, completed the required training, and been authorized by the OEC. Foreign nationals will only be authorized by OEC once any license requirements have been fulfilled through documentation of an applicable exemption or license exception, or by receipt of an approved export license.

Recordkeeping

US export control regulations require retention of records associated with all exports, use of license exceptions, and certain other activities. The Responsible Party or Department shall be responsible for keeping records for the required five years from the date of the last related activity or longer if necessary to comply with regulatory requirements or the terms and conditions of the award.

End of Project Requirements

Upon completion of this project all *Covered Items and Information* must be disposed of in accordance with applicable sponsor terms and US export control requirements. Hard copies will be disposed of by cross-cut shredding, incineration or return to the provider; an export license or other authorization may be required for foreign providers. Electronic files will be destroyed by using current "wiping" software. Contact OEC or your department information technology/security administrator for information on effective solutions for wiping. Hardware and equipment can be disposed of properly by contacting OEC; no *Covered Items and Information* may be surplussed without prior approval of OEC. This TCP must be maintained as long as *Covered Items and Information* are retained by UVA.

Associated Agreements

It is important that the OEC be able to link this TCP to any associated sponsored programs and other agreements to assure compliance with their terms and conditions. List all agreements, both funded and unfunded, associated with the acquisition and use of the Covered Items and Information in the table below:

#	Title or Description	Sponsor or Other Party	Type of Agreement	IT Security Clause (if any)	UVA Project-Award #
1			Select One		
2			Select One		
3			Select One		
4			Select One		
5			Select One		
6			Select One		
7			Select One		

Internal Notification & Assessment

Notification. The Responsible Person shall notify OEC (1) prior to adding new personnel; (2) when the scope of the project changes; (3) to request modifications to the approved TCP; and (4) when there is a change in funding, or in the award terms or conditions. The Department shall notify the OEC if (1) the Responsible Person resigns, retires or otherwise ends their employment at UVA; (2) if there is a change in the Principal Investigator on a sponsored award associated with this TCP; or (3) it becomes aware of any deviations from the requirements of this TCP.

Re-Certification. The Responsible Person shall certify annually, or at any time upon the request of OEC, to the following: 1) the accuracy of the TCP or if needed provide any necessary updates; 2) that all activities involving *Covered Items and Information* are being conducted in compliance with the approved TCP; 3) that all personnel have completed any required training; and 4) the current status of the project, i.e. completed or ongoing, which necessitated the development of the TCP. Failure to comply with requests for re-certification in a timely manner will result in revocation of approval and notification of the appropriate Department Chair, Dean, and Office of the VP for Research or Provost, as appropriate. Failure to comply with re-certification requirements or with the terms of the TCP may also result in denial of access to sponsored funds for work involving *Covered Items and Information* and may constitute a violation of US export controls.

Assessment. The Responsible Person and Department agree to cooperate fully with any compliance checks initiated by the OEC. Checks may be conducted for cause or as part of a random assessment process.

Submitted By: _____ Date: _____ Signature: _____

If submitted via e-mail from the Responsible Person's UVA account a signature is not required

OEC Approval By: _____ Date: _____ Signature: _____

OEC Assigned TCP # _____

Appendix 1 (required)
Personnel List

No.	Full Name	US Status	Country(ies) of Citizenship/Residency *(only required for Non-Immigrants)*
1		Select One	
2		Select One	
3		Select One	
4		Select One	
5		Select One	
6		Select One	
7		Select One	
8		Select One	
9		Select One	
10		Select One	
11		Select One	
12		Select One	
13		Select One	
14		Select One	
15		Select One	
16		Select One	
17		Select One	
18		Select One	
19		Select One	
20		Select One	

Appendix 2 (optional)
Additional Covered Items and Information

#	Name or Description	Type	Jurisdiction	Classification *
9		Select One	Select One	
10		Select One	Select One	
11		Select One	Select One	
12		Select One	Select One	
13		Select One	Select One	
14		Select One	Select One	
15		Select One	Select One	
16		Select One	Select One	
17		Select One	Select One	
18		Select One	Select One	
19		Select One	Select One	
20		Select One	Select One	
21		Select One	Select One	
22		Select One	Select One	
23		Select One	Select One	
24		Select One	Select One	
25		Select One	Select One	
26		Select One	Select One	
27		Select One	Select One	
28		Select One	Select One	
29		Select One	Select One	
30		Select One	Select One	