Technology Control Plan

TCP or Project Name (optional)**:**	

STATEMENT OF COMMITMENT:
The University of Virginia is committed to complying with applicable export control, embargo and trade sanction, and information security requirements in the conduct of university activities. This commitment is articulated in University policies, e.g., *FIN-043, Managing Export and Sanction Compliance in Support of University Activities* (http://uvapolicy.virginia.edu/policy/FIN-034) and *RES-009, Compliance with Sponsor Requirements* (https://uvapolicy.virginia.edu/policy/RES-009), and through the execution of awards and agreements that bind the University to specific contractual obligations, e.g., for safeguarding controlled unclassified information (CUI) (for more information see, http://export.virginia.edu/controlled-unclassified-information).

Information identified as requiring protection under a TCP is, at minimum, moderately sensitive data as defined University policy *IRM-003, Data Protection of University Information* (http://uvapolicy.virginia.edu/policy/IRM-003); in some instances, it may be highly sensitive data and/or require additional safeguarding, e.g., in order to prevent access by foreign persons.

A TCP must be maintained for as long as the covered items and information, identified in the TCP, require protection and are maintained by the University. This requirement applies regardless of funding status.

RESPONSIBLE PERSON:
A faculty member or executive who has oversight and responsibility for the underlying work. In the case of sponsored programs this should be the principal investigator unless an exception is granted by the Office of Export Controls.

Name:	
Computing ID:	
Department, Center or Unit:	

Once completed the TCP form should be submitted to export-controls@virginia.edu for review by the Office of Export Controls. Once the Responsible Person and Office of Export Controls agree to a final version, the Office of Export Controls will route it for electronic signature through DocuSign. Only TCPs signed by both the Responsible Person and the Office of Export Controls are considered approved. Subsequent modifications must go through the same review and approval process.

ASSOCIATED AGREEMENTS:
Identify all agreements, funded and unfunded, associated with the covered items and information identified below and protected under this technology control plan. *Provide the following information for each associated agreement.*

Type of Agreement	**ResearchUVA Project, Award, or Non-funded Agreement No.:**	**Sponsor or Other Party:**

SPONSOR/PROVIDER REQUIREMENTS:
Prior Approval: If the terms and conditions of a sponsored award or other agreement require prior notification and/or approval by the sponsor or provider for any export (or other release), the Responsible Person must work with the Office of Sponsored Programs to obtain such authorization prior to effecting the export (or other release). The Office of Export Controls review of the planned export and, if needed, submission of an export license application to the cognizant US government agency can occur concurrently with submission of the request to the sponsor.

COVERED ITEMS AND INFORMATION:
Identify the items or information that will be protected under this TCP. *Provide the following information for each individual or type of item or information that requires safeguarding. Control status means the applicable regulation or standard under which the covered item or information must be protected, e.g., ITAR (provide the USML category if known), EAR (provide the ECCN if known), or NIST SP 800-171 (CUI safeguarding).*

Name or Description:	**Type/Format:** *hardware, software, electronic information, hard copy documents, etc.*	**Source:** *provided by external party (provide name and relationship) or generated at UVA*	**Control Status (will be confirmed by OEC):**

SECURITY OVERVIEW:
The "one lock" principal is the minimum safeguarding required for all covered items and information, additional protections may be required depending on specific regulatory or contractual requirements. "One lock" means that at least one safeguarding mechanism will be in place to prevent individuals not identified and approved as part of this TCP from gaining access to the covered items and information. All project personnel are responsible for assuring that adequate safeguarding is maintained at all times.

PHYSICAL SECURITY:
Work Area: Locations where work with covered items and information will be performed must have restricted access. Restricted access is defined as having a clearly defined perimeter which is adequate to protect against oral and visual disclosures. Physical barriers are strongly recommended but are not required as long as oral and visual disclosure can be prevented, e.g., by the use of privacy screens on monitors. All project personnel within the restricted area are responsible for assuring that non-project personnel are excluded when work is being performed with covered items and information.

Building:	**Room number(s):**	**Specific Safeguards to be Employed:**

Physical Storage: Covered items, including hard copy documents, must be secured when not in the effective control of project personnel. Depending on the item(s) to be secured, safeguarding may be effected by a locked room, safe or other storage device/container as long as access is limited to project personnel. A locked room will not be sufficient if janitorial or maintenance staff have unrestricted access; in this case secondary containment such as a locked file cabinet or case will be required.

Building:	**Room number(s):**	**Specific Safeguards to be Employed:**

Marking: Whenever practicable, covered items and information must be clearly marked with their control status (e.g., CUI, ITAR, or EAR) and an appropriate warning provided. In the case of documents, this may be done using a cover sheet, watermark, or header/footer. Marking provides essential notification to project personnel about what items and information must be secured and is intended to prevent inadvertent access or release.

SECURING DIGITAL RESOURCES:
Desktop and Laptop Computers: All computers used to access or store covered items and information must be configured as high-security workstations (http://security.virginia.edu/elevated-workstation-privileges). As a general rule, only approved project personnel should be designated users of computers used to access or store covered items and information. *Note: Unless identified and approved as part of this TCP, administrative access by central, school or departmental IT personnel must be limited to US persons (citizens, permanent residents or protected individuals).*

List all Computers:	**List all individuals, whether or not they are project personnel, who will have administrative access (by device if appropriate):**	**Data Manager (Individual responsible for approving CUI going into and exiting Ivy-CUI environment), if applicable:**

Data Importation/Exportation Plan: Procedures securely moving information into or out of the controlled environment are critical aspects of a TCP and are essential for assuring the integrity of the data and the security of the UVA electronic resources used to store or process controlled information. *Note: If this project is subject to CUI terms, Globus is currently the only approved method for secure file transfer into or out of the Ivy-CUI environment. Use of another method or tool will have to be reviewed and approved by InfoSec and enabled by the Ivy system administrators.*

☐ **Globus** - Available whether or not the Ivy-CUI environment is used.

☐ **Other -** Provide a detailed description of how the covered information will be transferred into and out of the secure environment in the space below:

Data Storage/Processing Devices and Services: Servers, external portable hard drives, flash/thumb drives, cd/dvd, etc. used to store covered information must be University-owned, limited to use on this project, and employ at least 256-bit encryption. Cloud services must be provided under contract to UVA, or in the case of sponsored programs to the research sponsor, and providers must be contractually obligated to provide adequate security including, when necessary, limiting access to U.S. person employees or contractors.

List all Data Storage/Processing Devices and Services:	**List all individuals, whether or not they are project personnel, who will have administrative access (by resource if appropriate):**

Phones, Tablets and Other Devices: Devices other than desktop and laptop computers may only be used to access, collect, or store covered information if approved as part of this TCP. Such devices must employ mobile device management. To request use of phones, tablets or other devices, complete the following:

Device Type	**Mobile Device Software Management to be Used**	**Reason**

Email: Transfer of non-public technical information via email must be specifically described and authorized in this TCP.

Specific Information to be transferred	**Method of Encryption**	**Recipient Information**

Public Web Pages and Data Repositories: Covered items and information, including Controlled Unclassified Information (CUI) must not be posted or stored on publicly available platforms.

Disposition of Covered Items and Information: All covered items and information, both electronic and paper, must be securely deleted/discarded or returned to the sender via an approved transfer method. Cross-cut shredding is the required method of destruction for paper documents. Covered items and information must be securely deleted from electronic/digital devices according to the procedures detailed at http://security.virginia.edu/electronic-data-removal-procedures#Secure%20Deletion prior to their disposition or disposal.

PROJECT PERSONNEL:

Identification: All project personnel, including the Responsible Person, who require access to covered items and information must be identified, below. Only the Responsible Person may request changes to list of Project Personnel. *Provide the following information for each individual.*

Name:	**Computing ID:**	**Country(ies) of Nationality/Citizenship:**	**Type of Visa or Other Authorization, if Not a U.S. Citizen:**

Training: All project personnel are required to complete training appropriate to the covered items and information and any applicable regulatory requirements. As part of training, project personnel are made aware of their responsibilities for safeguarding covered items and information, preventing legal/regulatory violations, and reporting potential issues.

Screening: All project personnel will be screened against publicly available U.S. Government restriction, denial, and debarment lists; the University will comply with the specific terms of any applicable entry. In addition, project personnel with access to Controlled Unclassified Information (CUI) that must be safeguarded in accordance with NIST SP 800-171 are required to have undergone a background check that resulted in no significant/relevant findings that would disqualify them from access to CUI. See University policy *HRM-034, Background Checks and Ongoing Responsibility for Employees to Disclose Criminal Convictions* (http://uvapolicy.virginia.edu/policy/HRM-034), for additional information.

EXPORT CONTROLS: If the Office of Export Controls has determined that all covered information is not export controlled AND no exports of covered items are planned, mark N/A for all questions in this section; only the UVA Office of Export Controls may make this determination. *Note: All commodities (e.g., hardware, executable software, materials, etc.) are subject to export controls. Technical information, including source code, about commodities that are subject to restrictions on access or dissemination are also typically subject to export controls.*

Planned Exports: The shipment or transmission of export controlled items or information out of the U.S., including to the international space station or international waters, is an export and may require a license.

Describe Any/All Planned Exports of Covered Items and Information:

Covered Items/Information Proposed for Export:	**Recipient(s):**	**Reason for Release:**	**Proposed Date:**

Any release of export controlled information to a foreign national, whether in the US or abroad, is an export and may require an export license. Under the ITAR, providing a foreign person with access to controlled items (military and intelligence items) is also an export if it conveys controlled technical data or constitutes provision of a defense service.

Describe Any Planned Release(s) of Cover Items and Information to Individuals OTHER THAN Project Personnel (copy and paste headings as needed).

Covered Information Proposed for Release:	Recipient(s):	Reason for Release:	Proposed Date:

Export Review: The Office of Export Controls reviews all TCPs, including personnel lists, to determine 1) the export control status of covered items and information; 2) assess the applicability of license exceptions, exemptions, and general licenses; and 3) determine any remaining license requirements. Certain proposed activities or personnel may not be authorized unless and until authorization has been obtained from the cognizant US government agency(ies).

Recordkeeping: U.S. export control regulations require retention of records associated with all exports, use of license exceptions, and other activities. The Responsible Party shall keep records for the required five years from the date of last export-related activity or longer if necessary to comply with other regulatory requirements or the terms and conditions of any associated sponsored program.

ONGOING REQUIREMENTS:

Modifications: Any change to an approved TCP, including the addition of new personnel, requires the **prior approval** of OEC. Approval of new personnel will not be issued until

- identification has been verified;
- required training has been completed;
- clear screening restricted party screening has been completed;
- if required, clear background check results have been obtained; and,
- if applicable, all export control requirements have been fulfilled.

Re-Certification: The responsible person is required to certify the accuracy of the TCP at least annually. Failure to comply with requests to update or recertify in a timely manner will result in revocation of approval and notification to the appropriate chair, dean, and the Office of Vice President for Research or other executive official, as appropriate. Failure to comply with the terms of the TCP, including but not limited to recertification, may result in denial of access to sponsored program funds for work involving covered items and information, denial of future funding requests by the sponsor, and may constitute a violation of U.S. export controls which may result in the imposition of penalties, including fines and imprisonment.

SUBMISSION:

Once completed the TCP form should be submitted by the Responsible Person to export-controls@virginia.edu for review by the Office of Export Controls. Once the Responsible Person and Office of Export Controls agree to a final version, the Office of Export Controls will route it for electronic signature through DocuSign. Only TCPs signed by both the Responsible Person and the Office of Export Controls are considered approved. Subsequent modifications must go through the same review and approval process.

SUBMITTED BY:		**DATE:**	
OEC APPROVAL BY:		**DATE:**	
OEC ASSIGNED TCP#:			