Technology Control Plan

Statement of Institutional Commitment

George Mason University (Mason) is committed to complying with applicable export control, embargo, and trade sanction laws and regulations in all university activities. This Technology Control Plan (TCP) identifies the specific measures that will be taken by the Principle Investigator (PI) or other Responsible Person and all project personnel to ensure compliance with those requirements. We want this TCP to be as accurate as possible, so if there is any information that you do not understand, or that is inaccurate, please contact Mason's Director of Export Compliance and Secure Research. Any deviation from this TCP requires written prior approval from the Office of Research Integrity and Assurance (ORIA).

GMU PI/Responsible Person: **[insert name]**

GMU Organization: **[insert department, center, or other organization]**

Contact Information for PI/Responsible Person: **[insert phone, email, physical address]**

Administrative Contact: **[insert name and contact information for administrator]**

Funding Number: **[insert funding number if TCP associated with a sponsored program]**

Covered Items and Information

The following items or information have been determined to be subject to export control requirements which require that Mason place limitations on who may have access to or use the items or information (hereinafter "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 ORIA 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 of Item (For equipment, include manufacturer and model number. For software, list the name and version. For an export-controlled agreement, list the parties to the agreement and the general nature of the restriction.)	Reason for Control	Jurisdiction and Classification*
1			
2			
3			
4			
5			
6			
7			

*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.

As a result of this determination, the PI/Responsible Person, identified above, has worked with ORIA 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

<u>Work Area</u>. 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 and how restricted access will be implemented in those areas.]

<u>Storage</u>. 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 in use, and the method(s) of securing such items.]

<u>Marking</u>. 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 civil and criminal penalties for the university and/or individuals. Contact the Office of Research Integrity and Assurance at (703) 993-2308 or*

smacmich@gmu.edu, if you find this item/document unsecured. When physical space is limited, an abbreviated warning may be used, for example: *Export Controlled -- ITAR.* Water marks, 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. Some contracts require certain markings on documents. Check your contract to confirm that there is not a specific requirement.]

Information Security

Computer. All computers used to access or store Covered Items and Information must run Microsoft Windows 7 or 8, Vista, Mac OS X, or Linux with the latest security service pack and patches; similar requirements apply to servers and other devices. In general, 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 (e.g., US citizens, permanent residents, refugees, asylees). At this time, most Mason central servers may be accessed by foreign persons and cannot be used to store export-controlled data.

[Describe any security methods, devices or procedures that will be employed to assure computer security. List IT personnel with administrative access to the computer or server.]

Data Storage and Transmission. 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/SS L) or mailing a disk or flash drive are preferred methods of electronic transfers of Covered Items and Information.

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

Supercomputing and Cloud Computing. 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

Award Terms. 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, Mason 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, as above.

Nondisclosure/Confidentiality. In most cases, proprietary information provided to Mason 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 ORIA.

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

Unless specifically identified in this section, no export of Covered Items and Information is permitted under this TCP. This prohibition on exports includes, but is not limited to, "deemed" exports to foreign nationals in the United States, as well as the permanent or temporary shipment or transfer of Covered Items and Information out of the United States (export). Any export not authorized in this section must be submitted to ORIA for review. Authorization will not be given until all export control requirements are met.

[Specify any planned exports of Covered Items and Information.]

Special Notes

Use the space below to provide any project specific notes or clarifications, including any other project specific requirements or conditions.

Project Personnel Requirements

Identification: All project personnel needing access to Covered Items and Information must be identified on and sign Attachment A: Acknowledgement of Technology Control Plan. The PI/Responsible Person may request the addition or removal of project personnel at any time by contacting ORIA.

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 20 years and fines of up to $1M per violation) for failure to comply with US export control laws.

Screening. ORIA 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 PI/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 ORIA. Foreign nationals will only be authorized by ORIA 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 PI/Responsible Person and/or the GMU Organization 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 sponsor terms and applicable 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 ORIA for information on effective solutions for wiping. Hardware and equipment can be disposed of properly by contacting ORIA. This TCP must be maintained as long as Covered Items and Information are retained by Mason.

Associated Agreements

It is important that this TCP can be linked to any associated sponsored programs and other agreements to assure compliance with their terms and conditions. List all agreements, 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	Funding Number
1				
2				
3				
4				
5				
6				
7				
8				

Internal Notification & Assessment

Notification. The PI/Responsible Person shall notify ORIA: (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 GMU Organization shall notify ORIA if: (1) the PI/Responsible Person resigns, retires or otherwise ends their employment at Mason; (2) if there is a change in the PI/Responsible Person on a sponsored award associated with this TCP; or (3) it becomes aware of any deviations from the requirements of this TCP.

Certification. The PI/Responsible Person shall by 31 December confirm that the project is ongoing and that it is being carried out in compliance with the approved TCP. A TCP signed between October 1st and December 31st of the respective year shall not require recertification until the following calendar year, but recertification must occur no more than 15 months from the date that the TCP is initiated.

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

Submitted by: Date:

Signature: ________________________________

Organizational Approval By: Date:

Signature: ________________________________

ORIA Approval By: Date:

Signature: ________________________________

ORIA Assigned TCP #

Attachment A
Acknowledgement of Technology Control Plan

I hereby certify that I have read and understand the provisions of the attached TCP for **[Title of Project or Program]** and certify my intent to abide by its terms. I have been informed that I can be held personally liable if I export or unlawfully disclose, regardless of means or format, export-controlled materials to unauthorized persons or locations. I understand that my obligation to protect export-controlled materials continues beyond the end of my participation on this project.

I understand that individual per violation penalties of up to $1,000,000 and 20 years imprisonment are possible under US export laws. I have been informed that individuals, including complicit supervisors, companies, and institutions may be targeted in export enforcement investigations.

Print Name: ______________________________________ Organization: _____________________________

US Citizen ___ Green Card ___ Foreign National/ Country of Origin: _____________________________

Signature: ____ Date: _____________________________________

Print Name: ______________________________________ Organization: _____________________________

US Citizen ___ Green Card ___ Foreign National/ Country of Origin: _____________________________

Signature: ____ Date: _____________________________________

Print Name: ______________________________________ Organization: _____________________________

US Citizen ___ Green Card ___ Foreign National/ Country of Origin: _____________________________

Signature: ____ Date: _____________________________________

Print Name: ______________________________________ Organization: _____________________________

US Citizen ___ Green Card ___ Foreign National/ Country of Origin: _____________________________

Signature: ____ Date: _____________________________________

Print Name: ______________________________________ Organization: _____________________________

US Citizen ___ Green Card ___ Foreign National/ Country of Origin: _____________________________

Signature: ____ Date: _____________________________________

Attach additional pages as necessary.