Part I

TECHNOLOGY CONTROL PLAN

(TCP)

1. Purpose

George Mason University is committed to compliance with export control laws. The Principal Investigator (PI) of an export controlled Sponsored Project shall be responsible for complying with applicable export control regulations, and preparing and implementing a project-specific TCP. The finalized TCP shall be reviewed and approved by to the University Empowered Official for export controls. The individual responsible for and committed to ensuring compliance with this TCP is (*insert name of PI*).

This TCP will establish procedures to be followed during the course of Sponsored Projects subject to International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), Office of Foreign Asset Control Regulations (OFAC) and other applicable export control regulations.

2. Background and Description of the Use of Controlled Items and Information

(PI to insert information here)

3. Physical Security

(PI to insert description of how equipment, technology, data, and other controlled information will be shielded from unauthorized persons—including descriptions of relevant security systems, and other types of building access restrictions).

4. Information Security

In compliance with export control laws, George Mason University researchers are to ensure that sensitive digital research data is appropriately protected. All project data and other related digital materials will be strongly password-protected and encrypted using commercially available encryption technology. The computer(s) on which this data will be stored shall not be connected to any networks. When this computer has reached its usable life, the hard drive will be forensically erased or destroyed using hard drive destruction services.

(PI to insert an outline of additional measures that will be taken to ensure that information access controls will be utilized and the requirements are being met. This should include the use of passwords and encryption protection. Data discard procedures should also be included, as well as other plans for controlling access to information. These procedures should address system back-up, who will have access, transmission procedures, how computers storing sensitive digital data will be sanitized upon completion of the project, and other procedures necessary to provide the required security. Due to their portable nature, the use of laptops for storage of research data must be justified and will require additional security procedures.)

5. Personnel Screening

The names and nationalities of all personnel with access to the controlled technology shall be listed.

(PI to insert this information, including the proof obtained to verify US citizenship status)

6. Training and Awareness

All personnel with access to controlled information on this project must read and sign the "Briefing and Certification on the Handling of Export-Controlled Information" certification.

(PI to attach all executed Certifications to this TCP).

7. Compliance Assessment

As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are continually reviewed and findings are reported to the Empowered Official. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP must be cleared with the Empowered Official.

8. Project Termination

Security measures as deemed appropriate will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminated when the information has been destroyed or determined to no longer be export-controlled.

_____

Principal Investigator's Signature Date

Part II

Briefing and Certification on
The Handling of Export-Controlled Information

This project involves the use of Export-Controlled Information. As a result, the project implicates either the International Traffic in Arms Regulations (ITAR) under the jurisdiction of the Department of State, the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce, or the regulations of the Office of Foreign Asset Control (OFAC) under the jurisdiction of the Department of Treasury.

It is unlawful under ITAR to send or take export-controlled information out of the United States, **OR** to disclose or transfer, either orally or visually, export-controlled information to a foreign person *inside or outside* the United States, without proper authorization from the federal government. Under ITAR and EAR, a license may be required for foreign nationals to access export-controlled information. A foreign person is a person who is not a United States citizen or permanent resident alien of the U.S. *The laws make no exceptions for foreign graduate students.*

In general, export-controlled information means activities, items, and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application. It does not matter if the actual *intended* end use of export-controlled information is military or civil in nature.

Researchers may be held personally liable for violations of the U.S. export control laws. Both civil and criminal penalties, including incarceration, may be imposed for unlawful export and disclosure of export-controlled information. As a result, extra caution is required when sharing export-controlled technology with others. All technology generated from this project, including technical information, data, materials, software and hardware, must be secured from use and observation by unlicensed, non-U.S. citizens (including students).

Certification:
I hereby certify that I have read and understand this Briefing, and that I understand and agree to follow the procedures outlined in the Technology Control Plan. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export-controlled information to unauthorized persons.

_____

Name Date