Master Technology Control Plan for Export Controlled Information

Georgia Tech Research Institute

Copies to:
Research Security Department (RSD)
ray.kangas@gtri.gatech.edu
al.concord@gtri.gatech.edu
terry.culver@gtri.gatech.edu
bill.gregory@gtri.gatech.edu

Information Systems Development (ISD)
jeff.jenkins@gtri.gatech.edu
GTRI Lead CSRs
Revisions and Updates
(Posted after January 2017)

November 2017
- Updated international travel policies concerning email and use of exemptions
- General editing throughout the document to improve clarity

March 2017
- Revised training requirements to attend annual training class offered by ORIA

January 2017
- Added requirement to use two-factor authentication
# TABLE OF CONTENTS

I. PURPOSE ........................................................................................................................................... 4  
II. APPLICABLE REGULATIONS & POLICY .......................................................................................... 5  
III. SCOPE and APPROACH ..................................................................................................................... 5  
IV. INFORMATION SECURITY PLAN ........................................................................................................ 7  
V. PHYSICAL SECURITY PLAN .................................................................................................................. 8  
VI. INTERNATIONAL TRAVEL .................................................................................................................... 9  
VII. PERSONNEL TRAINING AND AWARENESS .................................................................................. 10  
VIII. SELF EVALUATION AND MANAGEMENT SYSTEM ........................................................................... 10  

Attachment A: Acknowledgement of GTRI Master Technology Control Plan for Export Controlled Information .................................................................................................................. 12
I. PURPOSE

The purpose of this “Master” Technology Control Plan (TCP) is to control the dissemination of Export Controlled (EC) information and items being utilized during the performance of Georgia Tech Research Institute (GTRI) projects or housed at GTRI.

This Master TCP shall be used for controlling export controlled project for GTRI personnel. An additional project specific TCP may be put in place when required.

This Master TCP shall be used to safeguard all GTRI information. A project specific TCP may be required if any of the following conditions exist on GTRI projects ineligible for Fundamental Research Exclusion (FRE):

a) Projects that require the use of Non-US Persons;
b) Projects that require the use of Students (including US citizens) for thesis or dissertation;
c) Projects that involve collaborative efforts with Resident Instruction facilities or labs (i.e. non-GTRI labs or participants).

Note: Projects that will export or share any export controlled information, technology, data, equipment or materials or services outside the USA – even to a US Military installation abroad – require a license or exemption. Please contact Export Office for licensing and/or exemptions prior to shipment. Please plan well ahead as some shipments, licenses or exemptions may require a significant lead time.

This TCP provides a roadmap for how GTRI will control these data, information or materials to ensure that unclassified export controlled information is not provided to Non-US persons (employees, students, colleagues or visitors) without the required export license from the Department of State and approval from the Offices of Research Integrity Assurance (ORIA) Export Team and Legal Affairs. Additionally, this TCP ensures that all individuals working on a project containing export controlled information understand their obligations under the export control laws and regulations. Disclosures of export controlled information to Non-US persons (whether he/she is an employee, consultant, sponsor, student, or visitor) is considered an export under the export control regulations and requires a license or other approval from the Department of State. Disclosures without the proper authorization can result in fines and jail time for the individual making the disclosure.

For contracts or projects that involve an OPSEC Plan/Concept of Operations (CONOPS), the Government or organizational protection/procedural guidelines (i.e., OPSEC Plans/CONOPS) that enhance the TCP requirements will be followed as directed by Research Security.

Please note: Non-US Persons may not be eligible to work on projects that do not qualify for the Fundamental Research Exclusion (FRE) without written approval from the Export Team/ORIA and, when required, a license from the federal government. Additionally, students (including U.S. persons) should not work on any project ineligible for the Fundamental Research Exclusion for their theses or dissertations. If a Non-US person or a student working on a thesis or dissertation is required for this project please contact the ORIA Export desk for assistance with obtaining appropriate approvals and preparing an individual TCP.
II. APPLICABLE REGULATIONS & POLICY

International Traffic in Arms Regulations (ITAR) 22CFR 120-130
Export Administration Regulations (EAR) 15CFR 730-774
National Industrial Security Program Operating Manual, (NISPOM), (DoD 5220.22-M)
Office of Foreign Asset Controls (OFAC)

POLICY

It is the policy of Georgia Institute of Technology (GIT) to fully comply with all applicable federal statutes, executive orders, regulations, and contractual requirements for the safeguarding of controlled technical information in its possession. This includes full and total compliance with export control regulations. Under no circumstances shall employees or other persons acting on behalf of GIT engage in activities in contravention of U.S. export control laws. Employees found to be in violation of these directives or the provisions of this plan may be subject to disciplinary actions, up to and including termination of employment. Such violations can also earn civil and/or criminal penalties for GIT and/or the individual making the disclosure.

The intent of this TCP is to demonstrate the appropriate level of security for controlled technologies as it pertains to export control requirements.

It is unlawful under the export regulations to send or take export controlled information out of the U.S.; or to disclose such information, orally or visually, or to transfer export controlled information to a Non-US person inside or outside the U.S. without proper authorization. A license may be required for Non-US persons to access export controlled information.

A Non-US person is a person who is not a U.S. citizen, alien who is a “Lawful Permanent Resident” (Green Card holder), (8 USC § 1101(a) (20)) or other “Protected Individual” under the Immigration and Naturalization Act (8 USC §1324b (a) (3)) designated an asylee, refugee, or a temporary resident under amnesty provisions. The law makes no exceptions for Non-US graduate students. Non-US Persons include any foreign corporation, business association, partnership trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

In general, the export of controlled information refers to the transfer/disclosure of items, materials, information, software, technology or other unclassified but restricted data to any person outside U.S. (including U.S. citizen abroad) or to any non-US Person inside the U.S. Export controlled information does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain.

III. SCOPE and APPROACH

The Project Director for each project is responsible for compliance with this TCP. It is applicable to all GTRI personnel producing or accessing export-controlled information or items and will include all operating locations, offices, temporary operating locations, and facilities whether located on campus or during visits to military reservations or in Government office buildings. Employees shall ensure compliance with the spirit and intent of the protection criteria contained herein and will be especially cautious when dealing with Non-US persons or entities, whether within the United States or abroad. This TCP has been put in place to ensure that transfers of export controlled items, materials, equipment, software, data, information or technology to Non-US persons does not occur without appropriate authorization. Each project will require adherence to the International Traffic in Arms Regulations (ITAR) under the jurisdiction of the Department of State, or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.
This plan is required because one or more of the following conditions exist:

**Export Controlled under a Classified Project:**
This project may involve classified information/equipment which, in itself, is export controlled. Handling of classified information is delineated in the NISPOM and this TCP does not modify the handling requirements for classified information. No release of classified information (i.e. confidential, secret, top secret) is permitted to any person without the proper security level clearance and a documented “need to know” for that specific information. The purpose of this TCP is to delineate the controls necessary for handling the unclassified export controlled items, materials, equipment, software, data, information or technology used on a classified project.

**Export Controlled under an Unclassified project:**
This project may involve access to unclassified export controlled items, materials, equipment, software, data, information or technology. The DFAR 252.204-7008 clause is to be used when the contract involves export controlled items or information. The clause states “… the parties anticipate that, in the performance of this contract, the Contractor will generate or need access to export controlled items.”

**Publication or Foreign National Restriction:**
The project may not involve export controlled items, materials, equipment, software, data, information or technology but a TCP is required due to a publication restriction or foreign national restriction. The Project Director and project participants may not release any information or publish results of the research without the prior approval unless the information or research results have already been placed (legally) in the public domain.

Non-US persons may not access this project without approval from the GIT ORIA Export Team and any necessary export authorizations from the federal government. It is essential to understand that if the project is controlled under ITAR, the Department of State must issue a license for Non-US persons to work on this project. The Project Director and all employees who have supervisory responsibility of non-US persons will be fully aware of their responsibilities regarding possible technology transfer and access control issues. In the event the project involves Non-US persons participating contact the ORIA Export Team for assistance with preparing an export authorization in the form of a license or exemption.

**NON-US PERSON VISITS OR CO-LOCATION OF NON-US PERSONS**
Non-US person may not receive or have access to export controlled information without appropriate export authorization (License or Exemption) and approval form the GT Export office. To ensure compliance with federal regulations and protect GTRI research participants from unintentional disclosures, controls must be in place to prevent an unintentional export to non-US persons. Non-US persons, including collaborators, visitors or tours, may not have access to GTRI facilities where export controlled research is conducted, including but not limited to research project data, information, materials, etc. without prior written approval from the ORIA Export Desk, an institute Empowered Official, and proper authorizations when required. A TCP or Technology Monitoring Plan (TMP) may be put in place to address the possible risk of an unintentional disclosure for any non-US Person or tour of the facility.

From time to time it is appropriate to co-locate a non-US Person within GTRI space or facilities due to research or programmatic needs. Prior to placement of any non-US person (paid or unpaid, employee or visiting scholar or guest) within GTRI facilities where export control research is conducted, an export review must be conducted to determine if any additional precautions or licenses are required. It is the responsibility of the Lab Director to contact the Export Desk at export@gatech.edu for prior written approval and when appropriate, an individual TMP for the non-US person or licenses if required.

GTRI personnel that find themselves working with or co-located with a non-US person are personally responsible for verifying that an export review has been conducted and the non-US person has been approved for the project and work location. GTRI personnel may contact their Lab Director or the Export Desk to verify Export review and approval for the non-US person. Any export controlled technical data, information, materials, etc. that are shared or provided to a non-US person without a license or exemption could result in an unlawful export requiring a Voluntary Self Disclosure.
IV. INFORMATION SECURITY PLAN

The following measures will ensure information security and will control access to computer systems and data:

Export controlled information may not be posted on networks with uncontrolled shared access.

Two-Factor Authentication:
Georgia Tech considers the security and privacy of employee and student information to be of utmost importance. Two-factor authentication is required of all faculty and staff when accessing campus services and systems that are integrated with the two-factor service. More information on the Two-Factor Authentication service can be found on the OIT website: https://twofactor.oit.gatech.edu. If your project contract requires two-factor authentication, this can be achieved by working directly with your IT support professionals and the Office of Information Technology.

Information Security
The protection of export controlled information residing on classified computers falls under the protection requirements of the NISPOM and are handled solely by the GTRI Research Security Department (RSD). Unclassified export controlled information residing on unclassified computer systems will be protected in accordance with the guidelines of this TCP.

Computers
All computers must contain the latest security service pack and patches for the OS. All unclassified systems will incorporate user identification and password protection as well as the use of generic GTRI and/or Lab firewalls to protect the information from internal and external unauthorized access. Passwords should be strong and at least compliant with current GTRI and GIT password policies.

Computers, Laptops, Tablets and Hard Drives taken off campus
All laptops, devices or equipment containing export controlled data that are taken off campus must provide physical access controls to prevent unauthorized admittance including a strong password and encryption. All encrypted systems should be encrypted by the unit CSR or designee and encryption passwords will be stored using a central key maintained by the CSR. Additionally, systems must be backed up on a regular basis due to the inherent risks of disk encryption. These backups should be monitored centrally by the CSR to ensure backups are successful. Visual access to the system monitor will be controlled in order to circumvent disclosure to unauthorized Non-US persons (such as closing the door, protect/shielding the screen, ensure only authorized people are in the room).

Note: Export Controlled Information may only be stored on GIT computers and networks. Never put export controlled information on your home computer or any public network.

Data Storage and Transmission
External hard drives or flash drive storage devices can easily be locked in a storage container, file cabinet or office when not in use. For data storage on drives with network access or backup servers, the controlled technical data files must be secured by encryption and password protection. These storage devices should not be considered “safe” for overseas travel; any export controlled information taken out of the United States of America on a portable storage device shall be considered exported. Export Controlled data may not be stored on non-GA Tech commercial Cloud or servers and may only be stored on GTRI servers approved for export controlled information. Non-GTRI servers, such as government servers/systems, may be approved once security protocols are confirmed. Contact your CSR, RSD or the export desk for assistance.

Email
Electronic communications involving export controlled information will be accomplished in accordance with established customer security requirements (e.g. using token request). Commercial encryption, user certification or other means of demonstrating “one-lock” control over the content of any email using or generating ITAR-restricted technical data should be used when specific guidance is not provided. Generally, emails from one GTRI account to
another GTRI account remain on the same server and do not leave GTRI and are therefore secure. Emails containing export controlled technical data being sent to non-GTRI email accounts should be sent as an encrypted attachment. Non-GIT email systems (Gmail, Yahoo, Hotmail, etc.) may not be used for export controlled data. Secure government addresses (.mil, .gov) may be used after verification of security protocols.

Physical Mail
Export controlled documents and material may be transmitted via first-class mail, parcel post or fourth-class mail (for bulk shipments). All international shipments on sponsored research projects must be approved by the ORIA Export Desk or the OLA. Biological and chemical shipments must be taken to Environmental Health and Safety (EH&S) for packing and shipping.

The following Destination Control Statement should be included by on international shipments:
“These commodities, technology or software were exported from the United States in accordance with the EAR or the ITAR. Diversion contrary to U.S. law is prohibited.”

V. PHYSICAL SECURITY PLAN

Buildings and work areas within GIT including GTRI Field Offices involved in classified work are protected in accordance with the guidelines of the NISPOM, incorporating such protective measures as card reader access, Non-US person escort requirements, spin dial door combination locks, video monitoring, and guard force presence as required by RSD. Unclassified export controlled information will be protected in accordance with the guidelines of this TCP.

The physical security of export controlled equipment and data will be ensured and shall be shielded from unauthorized persons. Non-US persons shall not have access to export controlled equipment or data without authorization by a valid export license.

Export controlled technical information, data, materials, software, or hardware, i.e.; technology generated from this project, must be secured from use and observation by unlicensed Non-US persons by being secured in a locked desk drawer, locked filing cabinet, or locked office. Security measures will be appropriate to the sensitivity involved. Non-US persons will be provided a segregated enclosed workspace and will be escorted or monitored by an authorized employee. Project Directors who have supervisory responsibility for non-US persons must receive an export control briefing that addresses relevant ITAR requirements as they pertain to export controlled information.

Conversations and Discussions
Conversations and discussions about the project or work products are limited to US Persons as defined in the US export regulations. Conversations and discussions shall be held only in areas where unauthorized personnel are not present. Conversations and discussions may not take place in public locations where non-US persons are present.

Presentations
Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations without prior approval of DDTC or BIS. Sponsored project agreements containing export controlled items, materials, equipment, software, data, information or technology may require that project personnel formally request and obtain prior government approval before the release of a publication or presentation. These requests shall be made in compliance with, and within the time frame stated in the sponsored project agreement. If no time frame is stated in the project agreement, three to six months may need to be anticipated for approval to be received from the contracting officer. Public release of information shall not occur until any required permission or other government approval is received by U.S. Department of State, Directorate of Defense Trade Controls, (DDTC), or U.S. Department of Commerce, Bureau of Industry and Security (BIS).
Publication
In most cases, restricted research will contractually require that project personnel shall not release or disseminate any information pertaining to the project without the prior written approval of the sponsor, excluding information already in the public domain. In the rare case that there is not a contractual publication restriction and the project involves controlled items, research results and publications generated from the controlled items are still subject to the approval of the sponsor. Therefore, when publications of projects that involve controlled items are subject to the approval of the sponsor, the impact of such restrictions should be considered prior to employing graduate students and tenure track faculty. Publications (including but not limited to, dissertations or journal publications) may be delayed or denied based on the approval of the sponsor or US government.

Marking of Unclassified Export Controlled Information
All technical documents that are determined to contain export-controlled technical data shall be marked “WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.” When it is technically not feasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the “Notice to Accompany Release of Export Controlled Data” required by DoD Directive 5230.25. If applicable, designated publication distribution statements shall be placed on the material.

Disposal
All physical items will be shredded, torn, or dismantled such that the controlled technology information contained within is indistinguishable. Files on hard drives will be deleted using appropriate sponsor approved measures. GTRI RSD destruction resources shall be used for properly disposing of controlled information and/or equipment located in the Atlanta area. GTRI Field Offices can also utilize this method of destruction if necessary.

Freedom of Information Act (FOIA) and GA Open Records Act (ORA)
As a public educational institution of the State of Georgia, GIT has certain obligations to respond to requests for “public” information. The Freedom of Information Act and applies to requests for information made to federal agencies and thus, GIT is not subject to FOIA. The state equivalent of the Federal act is the GA Open Records Act (ORA). The ORA provides that all citizens are entitled to view the records of state agencies on request and to make copies for a fee. The ORA requires that Georgia Tech produce public documents within three business days. If you receive a request for records under either Act, please contact the GT OLA immediately. Not all Institute information is subject to state statutes, and each request for information is reviewed by appropriate administrators and the GIT OLA for our legal obligations for release or protection of the information. GIT believes sufficient control and supervision will exist in regard to all employees, undergraduate and graduate students, including those with non-US person status, relating to technology transfer or release of technical know-how. It is the intention of GIT to protect all of its information not in the public domain unless appropriately authorized by a court of competent jurisdiction, applicable state statute, or the U.S. Government as may be required in each individual case.

In order for GIT to assume responsibility to meet federal regulations previously cited, no employee, graduate/undergraduate student, or other person acting on behalf of GIT shall disclose or release any export controlled technical data, items, materials, equipment, software, data, information or technology without full compliance with this TCP.

VI. INTERNATIONAL TRAVEL

Individuals may not take or work on export controlled projects/information when traveling abroad without prior authorization, when required.

a) Laptops, tablets, phones (including Blackberries, iPhones, smartphones, etc.) containing export controlled information may not be taken even if controlled information is encrypted or not accessed. In order to minimize the risk of unlicensed data export, the following options are recommended:
   i) Only take “clean” electronic devices (e.g., laptops, tablets, phones). These devices must not contain any unlicensed export controlled information, should be encrypted, and should only contain user data preferred by GIT. The devices are to be physically destroyed at the end of the project if unclassified, or disposed of through the use of approved methods.
necessary for the trip. GTRI can provide loaner electronic devices for international travelers including computers and smartphones.

ii) All devices (excluding GTRI-loaner devices) should be reviewed prior to departure to ensure compliance with export control laws including encryption regulations (submit to OLA via TAR prior to travel).

iii) Retain physical possession of all electronic devices while outside of the U.S.

b) If you need to check GTRI email while out of the country and you normally receive export controlled emails in your inbox, you must proceed carefully.

i) If you are travelling to a non-126.1 country, GTRI may be checked under the following conditions:
   1. You should purge your email folders of all ITAR before you leave. In general it is a good practice to not store ITAR and sensitive data in your email folders long term.
   2. You should only use the web interface to read your email. You can log on through https://mail.gtri.gatech.edu
   3. If you do receive an email that you believe may contain ITAR, you should delete it and not open the email. If you do this, no report is necessary.
   4. If you do accidentally open an email containing ITAR (thus downloading it in a foreign country), you must report this to Mary Beran in GTRC. Since you are not in a 126.1 country, it is not a major violation, but needs to be reported and logged.
   5. If you would like to use your mobile device (iPad, iPhone, android, ...) that is allowable as well. You must have AirWatch installed to connect to the server, which will ensure encryption on your device. The same rules for ITAR (#5 and #6) apply.

ii) If you are travelling to a 126.1 country, a travel email must be used. A CSR will set up a second account such as JohnDoe_in_China@GTRI.gatech.edu for you and put an out of office message in your normal account saying that Non-Export Controlled emails can be sent to the outside-the-USA address (JohnDoe_in_China@GTRI.gatech.edu). If you do retain and use your regular GTRI email address while on travel and receive export controlled information delete it immediately and inform RSD and Export as soon as practical.

More information can be found at: http://www.oit.gatech.edu/security-travel-tips-laptops.

VII. PERSONNEL TRAINING AND AWARENESS

Prior to participation on this Project, all participants (faculty, staff, students, contractors, etc.) shall attend an annual export training session to ensure compliance with the spirit and intent of the protection criteria contained herein and will be especially cautious when dealing with Non-US Persons or entities, whether within the United States or abroad. The PI of the project is responsible for ensuring all personnel working on the project complete required training. The Georgia Tech Research Corporation (GTRC), Research Security Department (RSD), in conjunction with the Office of Research Integrity Assurance, provide annual briefings to project personnel concerning the guidelines of this TCP as well as other categories of information protection required by the Department of State, the Department of Commerce, and Georgia Tech. Register for Export Control & TCP training at https://training.osp.gatech.edu. Refresher training will also be required throughout the life of the project.

All project personnel must read and understand this TCP, sign Attachment A, and attend Export Control Training to work on the project or be charged to it. Project personnel must be aware of their responsibilities to prevent inadvertent or other inappropriate disclosure of controlled items and of the personal criminal and civil penalties (including prison sentences of up to 10 years and fines of up to $1M) for failure to comply with U.S. export control rules. All project personnel will be screened against the applicable restricted parties’ lists. The Project Director is responsible for ensuring all new project participants have reviewed the TCP and attended training before allowing access to project items, materials, equipment, software, data, information or technology.

VIII. SELF EVALUATION AND MANAGEMENT SYSTEM

A thorough review of this TCP will be conducted by the ORIA, OLA and RSD on an annual basis to ensure compliance with federal security requirements and to determine whether changes, updating, or upgrading of the
TCP protective measures are warranted. Each GTRI Director will also initiate a periodic internal review of this TCP to ensure that the compliance system is operating effectively. If changes are required, the PI will forward proposed changes to ORIA and RSD for review and approval. The annual and periodic review will include a check of the project personnel listing, random personnel interviews, verification of physical security protective measures, and a review of the information security protective measures. A project specific TCP will be drafted if this TCP is unable to fully protect the information for the project.

REPORTING AND RESPONSIBILITIES

Any person having knowledge of a potential violation or noncompliance with the provisions of this plan or any applicable export control directive shall immediately report the circumstances surrounding the activity to the ORIA Export Desk and GTRI RSD. The reporting can be accomplished via the below listed points of contact. When appropriate, GIT shall disclose involvement in violations to the proper authorities in accordance with applicable regulations. Any deviation or waiver from or exception to these procedures requires prior approval of the signatories hereto. Any violation of the terms of this plan may be grounds for disciplinary action. Business managers must read the TCP and agree not to process a PSF to add non-US person personnel to applicable projects without the prior approval from the ORIA Export Desk.

All project participants must report any suspicious or unsolicited request for export controlled information by unauthorized persons. Unsolicited contacts can be in the form of email, personal or telephonic questioning. Unsolicited emails will be forwarded to suspicious.email@gtri.gatech.edu. Personal or telephonic queries can be reported through email descriptions of the query and unauthorized person involved. Regardless of whether the contacts seem suspicious they should be reported immediately.

reportacontact@gatech.edu should be used by all GT personnel in the Study Abroad, Work Abroad programs or Traveling Abroad.

CONTACT INFORMATION

Research Security: Export Desk:
Raymond J. Kangas Jr. Mary Beran, MA, CPIA
Technology Control Officer Director
GTRI Research Security Empowered Official
(404) 407-7132 (Office) (404) 385-2083 (Office)
(404) 407-9232 (Fax) (404) 385-2081 (Fax)
(404) 547-3520 (Cell) (404) 290-2160 (Cell)
ray.kangas@gtri.gatech.edu export@gatech.edu

Primary Point of Contacts: main email for all correspondences export@gatech.edu

Export Control:
Mary M. Beran, MA, CPIA
Director & Empowered Official
Office of Research Integrity
Georgia Institute of Technology
Office: 404.385.2083
Cell: 404.290.2160
mary.beran@gtrc.gatech.edu

Research Security:
Raymond J. Kangas Jr.
Technology Control Officer
GTRI Research Security
Office: 404.407.7132
Cell: 404.547.3520
Fax: 404.407.9232
ray.kangas@gtri.gatech.edu

Export Control:
Rhonda Shaner, M.Ed.
Research Associate
Office of Research Integrity
Georgia Institute of Technology
Office: 404.385.0288
Cell: 404.654.2910
rhonda.shaner@gtrc.gatech.edu

Export Website: http://www.export.gatech.edu/export-control
Attachment A: Acknowledgement of GTRI Master Technology Control Plan for Export Controlled Information

Acknowledgement of Technology Control Plan and Non-Disclosure Statement

I hereby certify that I have received, read, and understand the GTRI Master TCP for handling Export Controlled Information and the procedures contained in this TCP. I agree to comply with the restrictions contained herein and with U.S. Government regulations as they pertain to export controlled information. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export controlled information to unauthorized persons. I further understand that I must attend export control training before working on any export controlled projects and that I must complete annual training thereafter.

I hereby acknowledge and understand that any information related to defense articles on the U.S. Munitions List (Department of State) or articles restricted by EAR (Department of Commerce), to which I have access or which is disclosed to me in the course of my (employment-assignment-enrollment-visit) at Georgia Institute of Technology, is subject to export control under the ITAR or the EAR. I hereby certify that such data will not be further disclosed, exported or transferred in any manner to any non-US person or entity without prior written approval of the Office of Defense Trade Controls, U.S. Department of State for ITAR or the BIS, Department of Commerce for EAR. If I inadvertently export to an unauthorized recipient any controlled items, materials, equipment, software, data, information or technology received during my employment-visit-enrollment, I will report such unauthorized transfer promptly to the ORIA Export Desk and acknowledge the transfer to be a violation of U.S. Government regulations.

Print/Type Name: _________________________________ Date: __________________
GTRI Unit: __________________________________________
GIT/Kerberos ID: _________________________________________

☐ US Citizen
☐ US Person (under export regulations): Permanent Resident (Green Card holder)
Country of citizenship(s) (list all if multiple citizenships):

__________________________________________________________________________

Please note: Non-US Persons may not be included under the GTRI Master TCP. Additionally, students (including U.S. persons) may not work on any project ineligible for the Fundamental Research Exclusion for their theses or dissertations (student hourly work is allowable). If student involvement will be used for their thesis/dissertation, please contact the ORIA Export desk for prior approval.

Signature: __________________________________________

Return Signed Attachment A to:
Ray Kangas, GTRI RSD ray.kangas@gtri.gatech.edu
CC to Export@gatech.edu.