Old Dominion University
Old Dominion University Research Foundation
Technology Control Plan (TCP) and Certification

Part I: Required Information

Individual Requesting and Responsible for TCP	
Telephone Number	
E-mail Address	
Request Date	

Location(s) Covered by TCP	Room Number, Building, and Street Address:	
	(This box will grow as locations are added)	
Description of physical security measures included	Yes/No -	
Project Personnel	List Name(s) below:	List citizenship(s) / Permanent Res. Status with each name:
All personnel who will have access to export controlled subject matter (add additional rows if needed)	(This box will grow with names)	
Is sponsored research involved?	Yes/No -	
If yes, ODURF Project Number		
Identify sponsor		

Projected start date and end date of project	Start Date:	End Date:
Is a non-disclosure agreement involved?	Yes/No -	
If yes, identify the parties:		
Contact Information:		

Attachments	
Approved	____ Adam Rubenstein, Ph.D. Assistant Vice President for Research Compliance OR: ______________________________________ Julian Facenda Executive Director, ODU Research Foundation

Part II: Briefing and Certification on the Handling of Export-Controlled Information

This project involves the use of U.S. Export-Controlled information, equipment, or software. As a result, the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), or other U.S. Export-Control regulations apply to the project.

In general, "Export-Controlled" means that activities, items, information, technology, and software related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, processing, or use of a controlled item requires an export license , or license exception, to physically export from the U.S. **OR** to discuss with or disclose to a person who is not a U.S. citizen or lawful permanent U.S. resident. The ultimate end-use or end-user of the information, software, or item is **not** determinative of whether it is Export-Controlled.

Basic marketing information on function or purpose; general system descriptions; information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities; published information in the public domain; and published patent information **is not** Export-Controlled. Information developed as a result of fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published, without any publication restriction or pre-publication review requirement is **not** Export-Controlled.

It is unlawful to send or take Export-Controlled information, technology, software, or items out of the U.S.; or disclose, orally or visually (including by email, fax, phone, etc.), or transfer to a foreign person inside or outside the U.S. without prior authorization from the cognizant U.S. government agency. A foreign person is a person who is not a U.S. citizen or lawful permanent resident alien of the U.S. A person lawfully in the U.S. on a visa for work or study **is a foreign person**. The law makes no exceptions for foreign graduate students or visiting scientists.

Researchers may be held personally liable for civil or criminal violations of the U.S. Export-Control Regulations. As a result, you should be clear on the requirements and exercise reasonable care in using and sharing Export-Controlled information, technology, software, or items with others. This Technology Control Plan is to help you assess, address, understand your obligations, and control access to the Export-Controlled aspects of this project.

The security measures you design and implement should be appropriate to the type, nature, and level of Export-Controlled information, technology, software, and/or items involved in the project. Examples of appropriate security measures include (but not limited to):

- Project Personnel - Authorized personnel must be clearly identified.
- Laboratory "work-in-progress" – Plans to protect project data and materials from observation by unauthorized individuals. This would include operating in secured laboratory spaces or during secure time blocks when observation by unauthorized persons is prevented.
- Marking of Export-Controlled Information - Export-Controlled information must be clearly identified and marked as export-controlled with a legend appropriate to the applicable control.
- Work Products – Paper data, lab notebooks, reports, and research materials are stored in locked cabinets, preferably located in rooms with key-controlled access.
- Equipment, components, or other Items – Equipment, parts, components, or other tangible items and associated operating manuals, diagrams, etc. containing identified "Export-Controlled" information or technology are to be physically secured from unauthorized access.

- Conversations - Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.
- Phones, PDA's, Tablets, Computers, MP3 Players, and Other Personal Electronics – No Export-Controlled data or information should be loaded to, sent to, or stored on any personal electronic device. See the provision on Information Security below.

Department(s):	
Research Project Title:	ODURF Project No.:
Sponsor:	
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 TCP. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export-Controlled information, technology, software, or items to unauthorized persons.	
Signature:	Date:
Printed Name:	

(PRINT AND EXECUTE THIS **CERTIFICATION** FOR EACH PERSON WHO WILL HAVE ACCESS TO EXPORT CONTROLLED SUBJECT MATTER)

Part III: Technology Control Plan (TCP)

1 Commitment

Old Dominion University (ODU) and Old Dominion University Research Foundation (ODURF) are committed to export controls compliance. The Principal Investigator is responsible for implementation of technology control plans. The ODU Office of Research is responsible for assessing the adequacy of technology control plans, as applicable. The Export Control Officer is Adam Rubenstein. Julian Facenda, Executive Director, ODURF and Adam Rubenstein, Ph.D., Assistant Vice President for Research Compliance, are both Empowered Officials who may approve this Technology Control Plan. The Export Controls Officer is the main contact for export control issues.

The individual responsible for and committed to ensuring compliance with this TCP is:

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

Please provide a brief overview of the project. Describe what sensitive data and materials will be provided and how they will be delivered:

3 Physical Security

Please describe the physical security controls that will be used to prevent unauthorized access to secured areas and to protect project materials and computers. At a minimum, these controls should cover the bullet point items in Part II above and the following:

- Plans to project materials (physical or digital) and to ensure that project materials not leave the secured areas (including via the network).

- Plans to ensure that work for this project is done within secured areas.

- Plans for clearly marking all physical materials (e.g. hardcopy, removable media, etc.) as export-controlled, propriety, and/or subject to an NDA as appropriate. The plan should provide that materials be physically secured from access when not in use.

- Procedures to ensure that only project members are present in the secured areas when work on this project is being performed.

- Plans to prevent non-U.S. persons viewing or having access to any project data (physical or digital) or secured area (including maintenance, cleaning, and others).

4 Information Security

ODU rules require all researchers to ensure that digital research data is appropriately protected. ODU policy provides guidance on procedures for Information Technology Security Policy at https://www.odu.edu/content/dam/odu/policies/university/3000/univ-3505.pdf. Export-Controlled data are categorized under the Data Classification Policy as Sensitive data.

Please explain, in sufficient detail, what information security controls will be used to protect sensitive project data. At a minimum, your plan must comply with the bullet point items in Part II above and the following guidelines:

- Any requirements explicitly outlined in the contract/NDA, such as technology controls, data classification, encryption, network access (or lack thereof), non-disclosure, secure destruction, etc., must be adhered to at all times.

- Export controlled project data must not be sent unencrypted over any networks. All data stored on computers and removable media must be encrypted at rest, utilizing a whole disk encryption product wherever feasible. A list of approved encryption methods is available from ODU Information Technology Services (ITS) at https://www.odu.edu/about/policiesandprocedures/computing/standards/02/05.

- Project computers must be dedicated exclusively for work that is covered by a Technology Control Plan, and not be general-purpose machines.

- Project computers should not be Internet accessible except when explicitly allowed by the data owner, and only for the minimum duration necessary to complete the activities requiring Internet access.

- Project computers should be non-networked unless network connectivity is required for project work. If network connectivity is required, project computers should be configured to deny all non-essential inbound and outbound traffic. Network connectivity must be restricted to the maximum extent feasible. MAC addresses for all Ethernet and wireless interfaces must be provided to the Information Security Office.

- All computers must meet the security standards outlined in the Information Technology Security Policy, or have adequate compensating controls in place. Any exceptions to this policy must be documented via a Computer Incident Report http://occs.odu.edu/security/incident/form/ and approved by the ITS Information Security Officer.

- When project computers reach their usable life, physical media (e.g. hard drives, USB drives, etc.) must be forensically erased or destroyed using University service, available through ODU Information Technology Services, Technical Support Center at 757.683.3192, email itshelp@odu.edu for more information or visit www.odu.edu/ts/helpdesk.

5 Personnel Screening

All personnel with access to the controlled technology and their nationality are listed in the TCP Certification Form.

6 Training and Awareness

All personnel with access to Export-Controlled information, technology, software, or items on this project have read and understand the "Briefing and Certification on the Handling of Export-Controlled Information." Export control training modules are available and additional export control training for this project may be conducted by the Export Controls Officer. Additionally, all personnel with access to digital data/information stored on their university computer have read and agree to follow ODU policies and procedures for protecting sensitive data.

7 Compliance Assessment

As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the Export Control Officer at arubenst@odu.edu (757.683.3686) or to the ODURF Executive Director at jfacenda@odu.edu (757.683.4293, ext. 600). The Export Controls Officer and the Information Security Office may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the Export Control Officer.

8 Project Termination

Security measures will be required for Export Controlled information and items after the project termination. Please describe the security measures to remain in effect for Export Controlled information and items following termination of the project as well as the document retention and disposition plan to be followed:

9 Changes to Personnel

In the event that someone is added to the Project Personnel, please have them review the TCP and sign the Certification and provide the signed copy to ODURF. In the event that someone ceases to work on the project prior to project termination, please take appropriate measures such as collecting any keys to the work room and/or storage area, change electronic access code, and remove access to project computers and other electronic storage devices.