TCP Security Control Measures

Project or Activity

Project or Activity Title:____

PI or Activity Director:____

Associated NDA □NO □YES

eGC1:________________

Scope

Sensitive Unclassified Information (SUI) is defined as unclassified information that does not meet the standards for national security classification, but is pertinent to the national interests of the United States, and requires, under law or policy, protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Projects and activities which use, create or share SUI need to protect the SUI from unauthorized disclosure.

These measures apply to SUI provided by outside parties and sponsors to the University. These measures also apply to information, technology and material items created at the University and controlled under U.S. export control regulations. Such material may be created during the course of a project or activity lifecycle.

The PI or Activity director of the associated project must complete the information required on this form. If additional assistance is required please contact exports@uw.edu.

Project Information

Please provide a short explanation of the project to be performed and where it will be performed. Please indicate if any of the controlled items listed below will be used in foreign locations.

Controlled Items

All SUI must be properly identified, listed below, and marked with the appropriate control. If receiving SUI from an outside party or sponsor, request that the providing party identify material provided with the correct control.

Ultimately**, it is the responsibility of the PI to identify the control if any technology, software or other information before sharing or disseminating, regardless of whether the providing party has identified the control.**

All SUI has associated prescribed security measures based on federal policy or University policy, depending on the level and type of SUI. At UW, all SUI is considered either UW Confidential or UW Restricted, with UW Confidential imposing a higher threshold of security measures due to the increased sensitivity of the SUI.

Export-Controlled Hardware
This includes articles, materials, supplies and other tangible items. The Commerce Control List (CCL) and the United States Munitions List (USML) make hardware fairly easy to identify and is generally much easier to control.

You do not need to list general consumer goods controlled by the Export Administration Regulations (EAR) that can be purchased by anyone while in the US such as laptops, computers, mobile devices, medical equipment, or “off-the-shelf” supplies. If your tangible item is not easily found on the CCL and is a cutting edge innovation, a review by the Department of Commerce may be necessary before deciding whether it should be listed and security measures implemented for that item. Please consult with exports@uw.edu if this is the case.

> **Example**: An off the shelf laptop that can be purchased by anyone while in the US can be used and does not need to be listed. However, providing the technology on how to engineer and manufacture the laptop *may* be export controlled to specific end-users.
> See Supplement No. 2 to Part 774—General Technology and Software Notes.

All ITAR controlled defense articles must be listed below.

Export-Controlled Technology

Defined as specific information necessary for the “development”, “production”, or “use” of a product. May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

> General Technology Note (Supplement No. 2 to Part 774).
> The export of “technology” that is “required” for the “development”, “production”, or “use” of items on the Commerce Control List is controlled according to the provisions in each Category.
>
> Technology can be exported in the following ways:
>
> 1. Electronic: Sending or transmitting technical data and software Outside of the United States, or In the United States to a Foreign National.

2. Visual: Showing of technical details of export-controlled items to a foreign national
3. Oral: Talking about the technical details of export-controlled items to a foreign national
4. Shipment: Shipping items outside of the United States OR taking items while traveling to a foreign destination.

Most export-controlled SUI will fall into this category and must be protected from unauthorized access or dissemination. Please list all export-controlled technology that will be handled or developed for this project.

Export-Controlled Software
Defied as a collection of one or more "programs" or "microprograms". The software could be something that is used to test or manufacture an end item and its control will be related to the hardware category.

Commercial off-the-shelf software does not need to be listed below. Please list any new software that will be developed on this project.

For all items listed, include the item name, description, identifiers (i.e. document control number, manual title, etc.) and specific Export Control Classification Number (ECCN) or United States Munitions List (USML) ITAR Category number. If you need assistance in product classification please contact exports@uw.edu or use the online catalyst tool to self-determine. If export controls are *unknown* at this time and will be determined throughout the project please indicate by using TBD.

EXAMPLE:

ITEM SOFTWARE EXPORT CONTROL 5E991
DESCRIPTION Software for generating graphs of Underwater acoustic wave propagation

ITEM: EXPORT CONTROL:
DESCRIPTION:

ITEM: EXPORT CONTROL:
DESCRIPTION:

ITEM: EXPORT CONTROL:
DESCRIPTION:

ITEM: EXPORT CONTROL:
DESCRIPTION:

UW Information Classification	**UW Confidential** Security Measures **Export Controlled – EAR, ITAR**	
Access Eligibility	Limit access to export-controlled material to UW employees and students who are U.S. persons.	
	Export-controlled material may be made available to foreign persons by a case-by-case evaluation, and in accordance with any required data sharing agreement, export license, and documented license exception.	APS 2.10.4.c#4 APS 2.10.4.d
	Certain computing personnel, as identified by UW Human Resources, must complete a criminal background check.	APS 2.10.4.d APS 2.1.7.g.1
Security of Physical Information and Material Items	**Storage** Store export-controlled information and material items under lock. Only parties who are eligible to access the information or items may possess the key or combination to the lock.	DSS recommendation.
	Marking To the extent feasible, mark information and material items with a conspicuous marking identifying it as subject to export regulations and identifying the export classification. Tags, marked envelopes, or other containers may be used for items that cannot be easily labeled.	DSS recommendation; common FOUO control.
	Transmission Ship export-controlled information and material items via first class or fourth class mail, parcel post, or common carrier such as UPS or FedEx only to parties who are eligible to access the information or item.	DSS recommendation; common FOUO control.
	Disposal Return export-controlled information and material items to the source of the information or item, or dispose of documents by shredding or destroying (burning, pulping, etc.).	DSS recommendation; common FOUO control.
Security of Computers and Electronic Information	**Storage** Store computers, media, etc. that process or store export-controlled information in same manner as physical information when the resource is not in use to prevent unauthorized access, theft, tampering or destruction.	APS 2.10.3.d#9 MCSS 2.1 APS 2.1.7.e.1
	Marking To the extent feasible, mark electronic export-controlled information by placing conspicuous labels in file data or in file names that identify the data by its export classification. See Security of Physical Information for marking computers and media.	DSS recommendation; common FOUO control.
	General Computing	
	Limit login access to systems that process or store export-controlled information to authorized users.	MCSS 2.1
	The system must provide an access control mechanism that prevents unauthorized users from running programs or accessing export-controlled information, allowing the allocation of system and data resources to individual users.	APS 2.10 3.d#5 APS 2.1.7.e.1
	Export-controlled information should be encrypted at rest, including such information in system backups.	APS 2.10.4.d
	Restrict the loading of export-controlled information onto laptops, or other portable computing or data storage devices to unusual operational circumstances that require such action.	APS 2.10 4.c#3
	Export-controlled information stored on laptops or other portable computing or data storage devices must be password protected and should be encrypted, or equivalent access protection measures must be taken.	APS 2.10.4.c#3
	Operating systems and application software must be supported, patched and maintained at the most current level provided by the manufacturer. If secure versions of essential software are not available, restrict access to vulnerable services to trusted computers via host-based firewalls, network access restrictions, or secure network protocols.	APS 2.10.3.d#3 MCSS 2.1 APS 2.1.7.e.1
	Application software must not allow unauthorized access to export-controlled information.	APS 2.10.3.e MCSS 2.1
	Define and implement procedures to prevent and detect malicious software, such as the use of auto-updating antivirus software or system performance monitoring.	APS 2.10.3.d#8 MCSS 2.1 APS 2.1.7.e.1
	Implement backup procedures to ensure data integrity, system availability, and business continuity as required, with consideration to business and discovery purposes. Test the ability to recover information from backups regularly.	APS 2.10.3.c#10 APS 2.1.7.e.1
	The system must maintain a functioning and accurate system clock.	APS 2.1.7.e.1
	Clear export-controlled information stored in memory and on media using a one-time overwrite prior to release from secure control for maintenance, travel outside the U.S., reuse of the resource outside of the controlled project, or surplus.	DSS recommendation.

	System Management Well-trained personnel who are knowledgeable in data security practices manage the system to professional standards.	APS 2.10.3.d#2
	User Accounts	
	Access control measures must be documented, and implemented and maintained in compliance with the principle of least privilege and the principle of separation of duties. Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems. Access control measures must be audited for compliance at least every three years.	APS 2.10.3.c APS 2.10.4.d APS 2.1.7.d APS 2.1.7.g
	User accounts for system access must be based on a unique identifier.	APS 2.1.7.d
	User accounts should be limited to the minimum necessary.	APS 2.10 3.d#5
	Provide user accounts only to authorized users.	MCSS 2.1
	No guest, shared or general-purpose accounts should exist on the system. Shared accounts are allowed only as authorized by the system owner or operator, and only where appropriate accountability can be maintained.	APS 2.10 3.d#5 APS 2.1.7.d
	Configure user accounts with the least privilege necessary.	APS 2.10 3.d#5 (implicit)
	Maintain the number of administrator accounts at the minimum required.	APS 2.10 3.d#5
	Do not use administrator accounts when an account with less privilege can meet the need.	APS 2.10 3.d#5
	Do not grant accounts with substantial system-administration privileges to individuals who do not have UW faculty or staff appointments.	APS 2.10 3.d#5
	Authentication	
	Implement two-layer authentication.	APS 2.10 4.d
	Provide secure user authentication processes that protect passwords from interception.	APS 2.10 3.d#6, MCSS 2.1 APS 2.1.7.e.2
	Login controls are provided through the use of good passwords.	MCSS 2.1
	User passwords associated with administrative access meet complexity guidelines.	APS 2.10 3.d#7 MCSS 2.1
	Networking	
	Block or disable all unnecessary network services.	APS 2.10.3.d#8
	The system is protected by a firewall, or other protection or other port-blocking mechanism, especially during system installation, updating, or restoration. Servers: Limit inbound and outbound traffic to the essential service(s). Desktop/laptop: Limit unsolicited inbound connections.	APS 2.10.3.d#8 MCSS 2.1
	Data must be encrypted during transmission. Information must be encrypted and then transmitted, or transmitted via secure tunneling protocols, such as secure sockets layer (SSL), transmission layer security (TLS), secure copy (SCP), or secure shell (SSH) protocols. Use of the latest version of each secure tunneling protocol is recommended.	APS 2.10.3.d#8 APS 2.10.4.d
	Web application code, including applications that are linked to data bases or files that contain sensitive information, must meet the Open Web Application Security Project standards for secure coding.	APS 2.10.3.e APS 2.10.4.c#2
	Network-aware client software, such as web browsers and email readers, should block the automatic execution of attachments, graphical files, or other common carriers of malicious software.	APS 2.10.3.d#4
	Remote access must be restricted to sources within the campus network and/or two-factor authentication for secure remote access.	APS 2.10.3.d#6
	The system should display a security warning banner prior to initiation of the logon process. The warning banner must inform all users that the system or application being accessed is proprietary, that it should be accessed only by authorized users, and that system use is monitored for enforcement purposes.	APS 2.1.7.e.2
	Logging and Monitoring Security relevant events, such as authentication failures, account lockouts, and modifications of security software or settings, must be logged and periodically reviewed.	MCSS 2.1 APS 2.10.4.d APS 2.1.7.d
	Disposal Return export-controlled information to its source; or clear the device by performing a one-time overwrite of all addressable storage prior to release; or physically alter media to prevent recovery of export-controlled information.	DSS recommendation.
	Reporting Immediately report incidents that potentially impact the confidentiality of EAR- or ITAR-controlled information, such as theft, loss, seizure, compromise, suspected compromise, hacking, etc., to the University Facility Security Officer by email to uwfso@uw.edu or by phone to 206-543-1315.	APS 2.5

Project or Activity Specific Security Measures

The following security requirements are applicable to this project and/or activity and must be implemented through the duration of the project or use of the export-controlled information, technology and material items

Approved Security Measures

The security measures described in this document, minimum and specific, only pertain to the aforenamed project or activity. Such measures will be monitored and implemented by the Principal Investigator or Activity Director for the duration of the project.

NAME and TITLE
Principal Investigator or Activity Director

SIGNATURE **Date:**

APPROVED
Facility Security Officer, University of Washington

SIGNATURE **Date:**

APPROVED
Export Control Specialist, University of Washington

SIGNATURE **Date:**