UNIVERSITY of WASHINGTON

Technology Control Plan

Policy and guidelines for restricted projects and activities.

Table of Contents

1 INTRODUCTION

1.1 Purpose

University of Washington (UW) is committed to maintaining a teaching and research environment that is open to the free exchange of ideas among faculty and students in all forums—classrooms, laboratories, seminars, meetings, and elsewhere. Such an environment contributes to progress in all disciplines. To this end, University research endeavors are generally fundamental research.

However, at times the University conducts proprietary, restricted, and classified research under sponsorship of the U.S. Government and private sector organizations**.** Proprietary, restricted and classified research, as well as other activities carried out by the University, may involve the use or creation of Sensitive Unclassified Information (SUI).

This Technology Control Plan, or TCP, describes the security controls implemented by the University to manage SUI, as required by U.S. Government statutes, regulations and guidance.

1.2 Sensitive Unclassified Information

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.

The restrictions applicable to information that determine its status as SUI include the following (not an exhaustive list):

1.2.1 Export Controlled Information (including technology, data, and software)

Incoming and created information may be export controlled. Specific export-controlled items, software or technology are listed on either the Commerce Control List (CCL) or the United States Munitions List (USML). Broadly, defense articles or services are controlled by the International Traffic in Arms Regulations (ITAR) while the Export Administration Regulations (EAR) controls dual-use items. You may request the assistance of the Research Security Team with determining the export controls applicable to the information used on the project or with the activity, by contacting exports@uw.edu and requesting an export control determination.

1.2.2 Confidentiality Agreements (CDA) and Nondisclosure Agreements (NDA)

Nondisclosure and Confidentiality agreements entered into by the University of Washington apply to the research or activity taking place at UW. Principal Investigators or Activity Directors may not sign CDAs or NDAs on behalf of UW. NDAs and CDAs may include restrictions, for national security purposes, on information being shared with the University. These restrictions may limit accessibility of the

information or may restrict participation by individuals in future research involving the information.

1.2.3 Master Agreements and Master Contracts

The Office of Sponsored Programs (OSP) has the delegated authority from the Vice Provost for Research to review, negotiate and sign Master Agreements. Master agreements often include restrictive language that pertains to future work or task orders under the Master agreement, and the Master agreement is incorporated by reference in future order contracts.

1.2.4 Material Transfer Agreements

The responsibility to review, negotiate and sign MTAs is with the Center for Commercialization (C4C) and the Office of Sponsored Programs. Stand alone MTAs not linked to a sponsored research agreements are reviewed and signed by C4C. MTAs embedded in a sponsored research agreement or associated with sponsored research are reviewed and signed by the Office of Sponsored Programs. MTAs received by UW in order to receive material for use on a UW project or activity may contain restrictions on the accessibility or use of the materials shared, for national security purposes.

1.2.5 Purchase Orders and Invoices

Purchase Orders can be signed by the department ordering the items from outside vendors. Each department maintains its own PO form and database of ordered items. Associated invoices and other end-user agreement documentation from the vendor may indicate the controlled nature of the technology, software, or item received by the University. If a vendor or other Outside Party requires the University to sign written assurances pertaining to export-control compliance, please forward to exports@uw.edu for review and approval prior to accepting the controlled items or information.

1.2.6 Marking

Information that is controlled may not be subject to a contract or agreement, but the controlled nature of the information may be clear from markings on the information. For example, warning labels on incoming e-mail or markings on the cover, header, or footer of hard copy documents or materials may indicate a restriction on the dissemination or use of the information, for national security purposes.

1.2.7 Scope

This TCP applies to all University of Washington employees, students and outside parties at the University who will have or are within the possession, custody, or control of SUI. UW employees, students, and outside parties at the UW are required to follow all information security and privacy policies, standards, or guidelines established by the University.

1.2.8 Policy

All UW employees, students, and outside parties are required to comply with national security laws, rules and regulations, and University procedures set out in this Technology Control plan and implemented to protect SUI. University employees or students and outside parties at the University shall only allow access to SUI to Authorized Persons according to this TCP.

The Principal Investigator or Activity Director of specific sponsored projects or activities that involve SUI will be required to institute a Security Control Plan (SCP)specific to the project or activity involving SUI when:

- Projects or activities involve the receipt of SUI from an outside party or sponsor, such as via a nondisclosure agreement or sponsored research agreement;
- Projects or activities are not considered Fundamental Research; or
- Projects or activities involve technology and software associated with export-controlled equipment.

All projects or activities requiring a Security Control Plan must be registered with and approved by the Research Security Team. Any updates to the SCP must also be approved by the Research Security Team.

2 Security Control Plan

2.1 Control Plan

The Security Control Plan (SCP) is essential in outlining what type of SUI or export-controlled item(s) will be used or shared throughout the duration of the project.

The SCP is the backbone of the TCP in that it outlines who is working on the project, export licenses or license exceptions or other permissions that are being used, control measures to prevent unauthorized access and acknowledgments of responsibilities.

The Principal Investigator or the Activity Director will need to gather certain information about project or activity participants. The University has developed various forms to capture the essential information needed to mitigate risk to the project, activity and University.

The forms which are part of the Security Control Plan are as follows:

- Authorized Access Form
- Security Control Measures
- SUI Acknowledgement

Once a user has been authorized by the designated authority they can begin work on the project or activity requiring access to SUI.

2.2 Authorizing Access

Candidates to receive SUI may be UW employees, students, or outside party individuals/entities. Access may not occur until the individual is authorized to receive access. In order to authorize access, the following steps are followed:

- Identify Type of SUI
- Citizenship verification
- Restricted party screening
- Training
- Acknowledgement of responsibilities
- Licensing and/or permissions, as applicable

The Principal Investigator or Activity Sponsor initiates a candidate's individual access authorization by initiating an SUI Access Request Form. The SUI Access Request Form ensures that the steps outlined above and described more fully in this section, are completed. The Principal Investigator or Activity Director can authorize access once these steps are followed, without approval by the Research Security Team, except in these circumstances:

- The SUI is ITAR controlled

- An export control license is needed
- An export control license exception or exemption will be used

In these three scenarios, only the Research Security Team can authorize access to the SUI. If these circumstances exist, the PI or Activity Director should complete sections I, II, and III, and forward the Access Request Form to exports@uw.edu for review and access approval.

2.2.1 Type of SUI

In order to review access requests, the type of SUI must be identified.

Information restricted under an agreement

All unclassified information provided by an outside party or developed at the University under a sponsored research agreement, material transfer agreement, confidentiality agreement, or any other contractual arrangement*, and the agreement contains clauses restricting dissemination or publication of the information for national security purposes or there is restriction on transfer based on citizenship* qualifies that information as SUI. In these cases, the government or sponsor requires review and approval prior to sharing the information. The most common examples of this type of SUI is export-controlled information or information deemed sensitive for security purposes (such as "FOUO" or "OUO").

Information restricted based on markings/distribution limitation

Some information may be marked with U.S. Government distribution limitations, even if the contractual arrangement does not anticipate sharing of SUI. If an item or information is marked, the marking will usually indicate the type of SUI.

Unclassified information related to a classified contract

Finally, all unclassified information related with a classified contract that has not been approved for public release is considered SUI. Most commonly, the associated DD Form 254 will indicate the level of restriction and required permission needed before allowing access to the SUI.

2.2.2 Verify Citizenship

If the restriction on access is based on nationality (e.g. export-controlled) the Principal Investigator, Activity Director, or the UW organizational human resources representative reviews the candidate's proof of citizenship and completes Part II of the SUI Access Request. Proof of citizenship must be one of the forms described below.

Proof-of-citizenship documents:

- Birth Certificate
- Passport
- I-9 Form
- I-129 Form
- Naturalization Certificate
- Certificate of Citizenship
- Certificate of a Birth Abroad
- Permanent Resident Alien Card
- I-94, stamped with Asylee, Parolee, Refugee Asylum, HP, or PIP

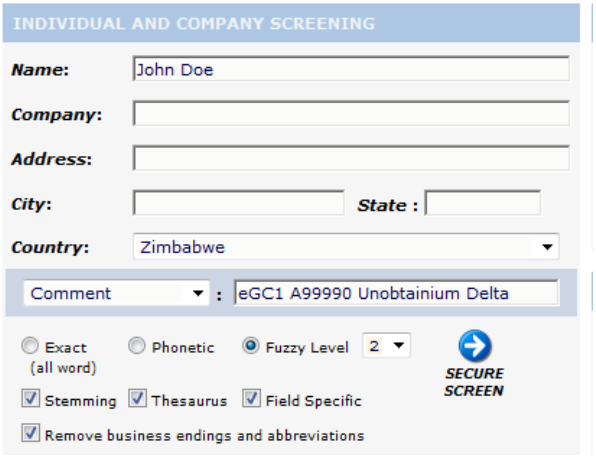
For Outside Party individuals, the Outside Party provides proof of citizenship to ensure that the University is obtaining necessary export licenses prior to allowing access. If the Outside Party is an entity, the business/institution's foreign location must be identified.

2.2.3 Screen for Federal Restrictions on Particular Individuals/Entities

The Principal Investigator, Activity Director, or his/her designee screens the name of a candidate (both individual and entity/institution name, if applicable) as found on the Access Request Form against restricted party lists to verify that the candidate is not ineligible to access the SUI and completes Part III of the Access Request Form. Any match of an individual or entity/institution name on a restricted party list will require consultation with the Research Security Team by contacting exports@uw.edu. The Research Security Team will assist with confirming a match.

To complete a Restricted Party Screening:

- Go to www.visualcompliance.com
  - Login with the **Username**: exports@uw.edu
  - and use the **Password**: RPS4UWPRJ
- Once logged in go to Restricted Party Screening (RPS) page and complete as many of the form fields as known.
  - At a minimum screen the business or individual **Name** and **Country** at a "Fuzzy Level" of 2.
  - Add a comment in the field related to the project (i.e. eGC1 or PI name etc..). This will provide a reference to the project or activity if a searched party is added or removed from restricted party lists.



- After the screen it is recommend you send yourself a copy of the results (See §3.1).
- Contact OSP for RPS results that *appear* to be positive for additional review.

2.2.4 Training and Awareness

All UW Employees or Students who will have access to SUI must undergo initial and periodic training on the handling of SUI. The level and frequency of the training will be dependent on the specific roles and functions of the individual as related to the project or activity. At a minimum, UW employees and students will be briefed in the definitions of fundamental research, export exemptions, exclusions, and licensing, as set forth by BIS and DDTC, which are pertinent to their activities. In addition to export control requirements, contractual and regulatory SUI requirements are covered.

Principal Investigators or the Activity Director will also undergo a briefing on their roles and responsibilities with regards to SUI, which includes but is not limited to: verifying citizenship, updating the Security Control Plan and submitting Access Request Forms, when required.

Outside Parties, when at the University and granted access to SUI, will undergo general training and awareness of their responsibilities with regards to SUI. This training is arranged with the Research Security Team on an as-needed basis.

2.2.5 Licenses and Permissions

Prior to sharing SUI, written authorization may be required from the respective cognizant agency.

For SUI that is export-controlled, this authorization may be in the form of an export license from the Department of Commerce; Bureau of Industry and Security (BIS) or the Department of State; Directorate of Defense Trade Controls (DDTC).

All other authorization to allow access to marked SUI that is not export-controlled or SUI related to a classified contract must be in accordance with the agreement under which the SUI is generated or

provided. Sharing of marked SUI that is not related to an agreement must be in the interest of the U.S. Government.

2.2.5.1 Export Control Licenses, Technical Assistance Agreements and Comprehensive Licenses

The Office of Sponsored Programs, Research Security Team prepares all export control license applications and other formal requests for approval to the Bureau of Industry and Security (BIS), the Directorate of Defense Trade Controls (DDTC) and the Office of Foreign Asset Controls (OFAC) for the University of Washington.

Export license(s) can be specific or broad to include the items, components, technology, or data that will be transferred. An export license may include components, systems, next higher assemblies (NHA) or the top level assembly.

In order to determine the need for a license, the Principal Investigator or Activity Director must provide specific technical information regarding the SUI in the Security Control Measures document and forward it with the Access Request Form to exports@uw.edu for review.

The licensing process for both BIS and DDTC can take 8 to 12 weeks therefore specific technology, information and data listed in the Security Control Plan must be provided as early as possible, in order for Office of Sponsored Programs to undertake a timely export control review and license or license exception determination.

2.2.5.2 Use of Exemptions or Exceptions in the ITAR and EAR

License **exemptions and exceptions** are available under certain circumstances. These types of permissions usually do not require notification to the regulatory agency but may require Electronic Export Information (EEI) to be filed through the Automated Export System (AES). A license exception or exemption may be used when a license would otherwise be required, but special circumstances warrant use of the exception or exemption. A license exception is specific to the technology, information or data, and destination. Use of exemptions requires specific certifications to be made by the exporter and in some cases, the recipient as well. In order to take advantage of the exception or exemption, specific documentation, describing how the criteria for the exception or exemption are met, is required in the Security Control Plan.

2.2.5.3 SUI Release Permissions (non-export controlled):

In situations in which the University is receiving outside SUI or creating SUI, approval for release must be obtained by the cognizant federal agency prior to sharing SUI. The permission requirements may be found in, but are not limited to:

- Associated agreements, such as a basic operating agreement
- A specific funding contract or a non-disclosure agreement
- DD Form 254, if associated with a classified contract
- Within applicable agency guidance such as the Information Security Program issued by Department of Defense (e.g. FOUO requirements in DOD 5200.1.R)

- On the SUI itself as a marking

Usually the Principal Investigator or Activity Director contacts the cognizant federal agency directly to obtain permission to release SUI. The permission obtained should be noted on the Access Request Form prior to sharing SUI.

2.3 Security Control Measures

Security Control measures provide basic and enhanced protection guides for storing and safeguarding SUI. The Principal Investigator or Activity Director of the project or activity is required to institute such measures. Control Measures are reviewed by the Research Security Team and, when approved, are associated to the specific project or activity.

Security control measures for information, technology, software or hardware are either recognized as UW Restricted (proprietary) OR UW Confidential (export-controlled). The security measures provide specific guidance on access, physical/electronic security and reporting requirements. These measures are based on UW policies and standards as found in APS2.1, APS2.5 and the Minimum Computer Security Standards. If there additional security requirements due to the nature of the work or the participation on the project, this is reflected on the Security Control Measures document by the Research Security Team.

Approval of the security measures is dependent on receiving the necessary information in order to assess the security requirements needed for the project or activity. Updates to the security measures may be needed as personnel are added or new SUI is added to the project. Please consult with exports@uw.edu if you have any questions.

2.4 Acknowledgement

UW Employees and Students must agree to the conditions and responsibilities of this TCP via the Acknowledgement Form, which is maintained by the PI or Activity Director with the project file.

For Outside Parties, the University requires that the recipient acknowledges, in writing, the receiving party's responsibilities to control access to the SUI. Access to the SUI by the Outside party is not allowed until this acknowledgement is received by the Principal Investigator or Activity Director responsible for the SUI.

2.4.1 SUI Access Acknowledgement – Campus

This form is tied to the project or activity where the project member acknowledges that they understand they are working with SUI, they have received training on how to protect it, and will inform supervisor(s)

of unauthorized access or distribution.

2.4.2 Sensitive Unclassified Information Acknowledgement – Outside Party

If you anticipate that you will share SUI with an outside party, the party must complete the acknowledgement form. The purpose of the acknowledgement is to ensure that the receiving party is aware that protection measures should be taken to prevent any unauthorized distribution. The acknowledgement also ensures the receiving party understands that under federal requirements, the steps of screening end-user(s) and adhering to US export control laws and regulations is the receiving party's responsibility once the SUI is provided from the University.

3 Procedures

3.1 Recordkeeping

It is the responsibility of Principal Investigator or Activity Director to maintain records of pertinent information related to this TCP. If related to a sponsored project, the TCP record must be kept in conjunction with the departmental grant and contract file. Records to be retained include but are not limited to:

- Export control documents and determinations, including signed Access Request Forms
- All manufacturing notes or acquisition information of the SUI
- SUI specifications
- Correspondence
- Requests for Proposal (RFP)
- Program Announcements (PA)
- Contracts, Awards, Task Orders and other funding instruments
- Financial records
- Licenses (applications, license approval)
- Use of license exemptions and exceptions
- SUI provider permissions and other sponsor requirements
- Exemption and Exception Certifications
- Export Transaction Records

Records must be maintained by the Principal Investigator or Activity Sponsor according to US Export Laws and Regulations for five (5) years and, if pertaining to a sponsored project, seven (7) years. Records are encouraged to be maintained electronically and must be capable of being reproduced on paper.

3.2 Reporting

Any suspicious behavior, misrepresentation, possible compromises and/or violations related to the security of SUI must be reported. Additionally, individual researchers/exporters are to report suspected violations of export control regulations to the Research Security Team or directly to the Empowered Official for investigation and self-reporting to the cognizant agency. The Empowered Official is responsible for reporting any possible ITAR violations to DDTC.

No person may cause or aid, counsel, command, induce, produce or permit the doing of any act prohibited by US export laws and regulations.

3.3 Monitoring Compliance

You may be held personally liable for violations of the ITAR and EAR and/or NISPOM. As a result, you should exercise care in using and sharing SUI with others. SUI must be handled in accordance to the security plans and/or controls specified in the TCP and only shared with individuals authorized to access the SUI as set out in the TCP.

Internal monitoring of the implementation of controls set out in the Security Control Plan is carried out by the individual PI or Activity Sponsor on an on-going basis.

Reviews of compliance with this TCP and the Security Control Plan per project or activity are carried out by the Research Security Team on a periodic basis.

Audits of the overall compliance program specific to this TCP is undertaken by the Research Security Team on a bi-annual basis to ensure the program is consistent with national security regulations.

3.4 Sanctions and Penalties

If US export or security laws or procedures are violated, the Empowered Official will consult with the Provost's office and other officials to determine appropriate actions and sanctions. Personnel sanctions may range from letters of reprimand to dismissal from UW employment. Personnel sanctions may also include restrictions of access to specific UW buildings or an outright ban from all UW campuses.

ITAR and EAR violations - $1,000,000 per violation and up to 20 years imprisonment. Suspension, debarment, or other civil penalties may be imposed.

3.5 Contacts

The Office of Sponsored Programs has been charged with the responsibility in establishing standards and monitoring Export Compliance for the University of Washington. General questions in regards to export-controls and US regulations should be addressed to exports@uw.edu.

If you have a specific question please call:

Robert (Bob) Conley
Research Security Specialist
conler@uw.edu
(206) 543-3214

Carol Rhodes
Associate Director
Office of Sponsored Programs
carhodes@uw.edu
(206) 543-2139