**The University of Iowa**

**Division of Sponsored Programs**

**Technology Control Plan (TCP) Certification**

**Part I**

|  |  |
| --- | --- |
| Individual Requesting and Responsible for TCP |  |
| Telephone Number |  |
| E-mail Address |  |
| Request Date |  |
| Description of Controls (EAR/ITAR Category) |  |
| Location(s) Covered by TCP(add additional rows if needed) | Building: |
| Office: |
| Project Personnel | List Name(s) below: | List citizenship(s) / Permanent Res. Status (with country of origin if not a US citizen): |
| Personnel who will have access to export controlled subject matter (add additional rows if needed) | Name 1Name 2Name 3This box will grow with namesName 4Name 5 | StatusStatusStatus |
| Is sponsored research involved?  | Yes/No - |
| If yes, identify sponsor |  |
| Sequence # |  |
| Projected start date and end date of project | ­­­­­­­­­­­Start Date: End Date: |
|  |  |
|  |  |
|  |  |
| Attachments |   | 1. TCP2. Export Briefing and Certification Form(s) for each person subject to this TCP |
| Approved | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Departmental Executive DateDean Date  AND:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Jennifer Lassner Date Empowered Official for Export Controls | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date of full approval  |

**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.

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.

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  **are 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.

The security measures you design and implement should be appropriate to the type, nature, and level of Export-Controlled information, technology, software, and/or other items involved in the project. . The following aspects should be considered, and those relevant to the project must be addressed with appropriate security measures in Part III: Technology Control Plan (TCP).

* Project Personnel - Authorized personnel must be clearly identified and receive approved export control training. Consider personnel with access to the project areas who are not directly involved in the project.
* Laboratory “work-in-progress” – Plans to protect project data and materials from observation by unauthorized individuals. This would include operating in physically secured laboratory spaces or during periods of time 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 should be limited to the identified contributing investigators and 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:  | Sequence #:  |
| 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Printed Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  | Date:  |

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

**To be completed by Export Control Coordinator:**

Restricted Party Screening completed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Date

Export Control Training Attended:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Date

**Part III: Technology Control Plan (TCP)**

# 1 Commitment

The University of Iowa is committed to export controls compliance. The Division of Sponsored Programs is responsible for implementation of technology control plans as applicable. Jennifer Lassner, Executive Director for Division of Sponsored Programs (DSP) is the Empowered Official. The Export Control Coordinator, Pat Cone-Fisher, (patricia-cone-fisher@uiowa.edu (319) 335-3582) is the main contact for export control questions.

 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 information technology. At a minimum, your description must cover the following items:

* Protection of the materials and methods to ensure they do not leave designated secure areas.
* Ensuring that work for this project is done within secured areas, and that only project members are present when work is being done.
* Clearly marking all physical materials (e.g. hardcopy, removable media, etc.) as export-controlled, proprietary, and/or subject to a non-disclosure agreement (NDA) as appropriate. The plan should provide that such materials be physically secured when not in use.
* Prevention of non-U.S. persons viewing or having access to any project materials or information (physical or digital).

|  |
| --- |
|  |

# 4 Information Security

The University of Iowa requires all researchers to ensure that sensitive digital research data is appropriately protected. The University of Iowa provides guidance on procedures at <http://itsecurity.uiowa.edu/resources/documents/security-overview.pdf>

Export-Controlled data are categorized under the Institutional Data Access Policy as Level III (confidential/restricted) data. See http://cio.uiowa.edu/policy/policy-InstitutionalDataAccess.shtml

Please explain, in sufficient detail, what information security controls will be used to protect sensitive project data. At a minimum, your plan must address the following IT security policy and 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.
* User activity and project data must be sent securely (encrypted) over any networks. All sensitive data stored on computers and removable media must be encrypted at rest, wherever feasible.

User activity and security relevant events must be recorded/logged on systems, and monitored for suspicious activity.

* Account passwords must comply with <http://cio.uiowa.edu/policy/Enterprise-Password.shtml>
* Project computers should not be networked or Internet accessible unless allowed/required by the research contract/grant. If project computers are to be Internet accessible, operating system and application patches must be applied in a timely manner (at least monthly), and configured for automatic updates, if possible. Project computers must be configured to deny all non-essential inbound and outbound traffic, and University recommended anti-virus and anti-malware must be used on all eligible devices.
* Systems must be registered with the Information Security & Policy Office so they can be regularly scanned for vulnerabilities. See <http://itsecurity.uiowa.edu/usr/>
* Any suspicious activity, or suspected (or confirmed) information security incidents must be immediately reported to the Information Security & Policy Office at 335-6332 or it-security@uiowa.edu
* When project computers are decommissioned, physical media (e.g. hard drives, USB drives, etc.) must be disposed of in accord with <http://cio.uiowa.edu/policy/ComputerEquipmentDisposal.shtml>
* Provisions for adequate backups, and recovery procedures for all project information must comply with <http://cio.uiowa.edu/policy/policy-backup-recovery.shtml>

|  |
| --- |
|  |

# 5 Personnel Screening

All personnel with access to the controlled technology and their nationality are listed in the TCP Certification Form and a Restricted Party Screening has been completed. No visitors shall be allowed access, including visually, to the secured areas listed in Section 3 without prior approval of the Export Control Coordinator.

# 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 for this project shall be conducted by the DSP Export Control Coordinator. No person shall have access to Export-Controlled information, technology, software or items on this project until such training is completed. The DSP also provides periodic training sessions to members of the University of Iowa community.

# 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 Coordinator at patricia-cone-fisher@uiowa.edu (319) 335-3582, or to the Executive Director for Division of Sponsored Programs at jennifer-lassner@uiowa.edu (319) 335-2123. The Export Control Coordinator and the Information Security & Policy Office may also conduct periodic evaluations and/or training to monitor compliance with 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 Coordinator or the Executive Director for the Division of Sponsored Programs and noted by a modification to this TCP.

# 8 Project Specific Export Authorizations

Unless specifically identified in this section, no export of export control listed material is permitted under this TCP. This prohibition on exports includes, but is not limited to, exports to foreign nationals in the U.S., as well as the permanent or temporary shipment or transfer of export control listed material out of the U.S. (export). Any export not authorized in this section must be submitted to the Export Control Coordinator for review; authorization will not be given until all export control requirements are met.

# 9 Internal Notification & Annual Recertification

Notification: The PI and department shall notify the Export Control Coordinator (1) prior to adding new personnel; (2) when the scope of the project changes; (3) to request modifications to the approved TCP; and (4) when there is a change in funding or in the award terms or conditions. In the event of a suspected violation of the export control regulations, please contact the Export Control Coordinator or the Office of General Counsel.

Certification: The PI shall certify, by 31 March annually, and the Export Control Coordinator shall confirm that the project is being carried out in compliance with the approved TCP. A TCP signed between January 1st and March 31st of the respective year, shall not require recertification until the following calendar year, but must occur no more than 15 months from the date the TCP is initiated.

# 10 Project Termination

Security measures will be required for Export Controlled information and items after the project termination. Export Control documents should be retained for 5 years unless directed otherwise by the applicable agency. The University of Iowa Records Management Policy may be found at <http://www.uiowa.edu/~our/opmanual/v/17.htm#173>. Describe any data retention requirements (Data Management Plan) that must remain in effect for Export Controlled information and items, as well as the on-going security measures that will be in place following termination of the project:

|  |
| --- |
|  |