|  |
| --- |
| Statement of Institutional Commitment |

Southern Illinois University is committed to complying with applicable export control laws and regulations in all university activities. Federal laws and regulations, including, but not limited to, the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) regulate the transfers of items, technology, software, technical data, and information to certain non-U.S. persons and entities.

It is unlawful under the EAR and ITAR to send or take physical items, technical information, data, products, software, hardware, biological materials, or chemical materials, hereafter referred to as “*export-controlled items and information*” out of the U.S. without proper authorization. This includes disclosing information orally or visually or transferring *export-controlled items or information* to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, an export license may be required for foreign nationals to access *export-controlled items and information*. A foreign person is a person who is not a U.S. citizen, a U.S. permanent resident or a person who is protected under the U.S. refugee and asylum status. The law does not make exceptions for foreign students.

All SIU employees and students are responsible for the export control implications of their work. They must ensure that their activities are in compliance with export control laws and regulations. Non-compliance carries severe institutional and individual consequences, including the loss of research funding, loss of export privileges, and/or criminal and civil penalties.

The project/activity named in the Program Information section below involves the receipt and/or use of *export-controlled items and information*. Such items must be secured from use and/or observation by unlicensed non-U.S. persons. This document serves as a template for the elements of a Technology Control Plan (TCP) and the safeguard mechanisms that need to be put in place to protect against unauthorized access or use. Security measures and safeguards shall be appropriate to the export classification involved.

This TCP identifies the specific measures that shall be taken by the Responsible Person. This should generally be the principal investigator unless approval is obtained from the Export Controls Office. It is the responsibility of the Responsible Person to provide true, accurate, and complete information requested within the TCP and to strictly adhere to the security measures established in this TCP. The Responsible Person is also responsible for informing the SIU Export Controls Office immediately after any changes to the information provided in this TCP becomes known to the Responsible Person.

|  |  |
| --- | --- |
| **Responsible Person:** | Click or tap here to enter text. |
| **Unit:** | Click or tap here to enter text. |
| Program Information | |

|  |  |
| --- | --- |
| **Project Title** | Click or tap here to enter text. |
| **Project Description** | Click or tap here to enter text. |
| **Principal Investigator** | Click or tap here to enter text. |
| **PI Phone Number** | Click or tap here to enter text. |
| **PI Email Address** | Click or tap here to enter text. |
| **Unit** | Click or tap here to enter text. |
| **Sponsor** | Click or tap here to enter text. |
| **Start Date** | Click or tap here to enter text. |
| **End Date** | Click or tap here to enter text. |
| **Award Number** | Click or tap here to enter text. |
| **Account Number** | Click or tap here to enter text. |

|  |
| --- |
| Personnel Screening and Training/Awareness |

Individuals who have access to *export-controlled items and information* must be screened against the various U.S. government denied parties/entities lists. Restricted Party Screening shall be performed by the SIU Export Controls Office using export control screening software licensed to SIU. Screening results shall be maintained as part of this TCP. If an individual or an entity is on a list, the Empowered Official shall evaluate the situation. An export license may be required for the person to participate, which could be denied.

Authorized project personnel are required to complete an initial in-person export control training when this TCP is implemented and are required to follow up training annually. The Export Controls Office shall monitor compliance with the TCP and confirm its accuracy on an annual basis with the PI. It is the PI’s responsibility to contact the Export Controls Office if any changes need to be made to the TCP during the course of the year. Once this TCP has been approved by the Unit Head and the Export Controls Office, the Responsible Party must complete and sign the Responsible Party Certification found in Appendix A.

The PI/Responsible Person is required to brief all participants on the requirements of this TCP. Each participant is required to complete and sign the Participant Briefing and Certification located in Appendix B.

**Project Personnel:** Complete the below information for each individual as it relates to the *export-controlled items and information*. Additional Project Personnel may be listed in Appendix C if necessary.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Name** | **Country of Citizenship** | **Role Related to Controlled Item** | **Date Screening Cleared** |
| 1 | Enter text. | Enter text. | Enter text. | Select a date. |
| 2 | Enter text. | Enter text. | Enter text. | Select a date. |
| 3 | Enter text. | Enter text. | Enter text. | Select a date. |
| 4 | Enter text. | Enter text. | Enter text. | Select a date. |
| 5 | Enter text. | Enter text. | Enter text. | Select a date. |
| 6 | Enter text. | Enter text. | Enter text. | Select a date. |
| 7 | Enter text. | Enter text. | Enter text. | Select a date. |

|  |
| --- |
| Export-Controlled Items and Information |
| The following items or information have been determined to be subject to export control requirements which require that SIU place limitations on who may have access to or use the items or information. Only those individuals who are identified below and have been approved by the Export Controls Office may have access.  Additional *Export-Controlled Items and Information* may be listed in Appendix D if necessary.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **#** | **Name of Item or Information** | **Type** | **EAR or ITAR?** | **Classification\*** | | 1 | Enter text. | Choose an item. | Choose an item. | Enter text. | | 2 | Enter text. | Choose an item. | Choose an item. | Enter text. | | 3 | Enter text. | Choose an item. | Choose an item. | Enter text. | | 4 | Enter text. | Choose an item. | Choose an item. | Enter text. | | 5 | Enter text. | Choose an item. | Choose an item. | Enter text. | | 6 | Enter text. | Choose an item. | Choose an item. | Enter text. | | 7 | Enter text. | Choose an item. | Choose an item. | Enter text. |   ***\*Provide the applicable U.S. Munitions List category and subparagraph if subject to the ITAR or the Export Control Classification Number (ECCN) if subject to the EAR.*** |
| Physical Security Plan |

Project data and/or materials must be physically protected from observation by unauthorized individuals by operating in secured laboratory spaces or during secure time blocks when observation by unauthorized person is prevented.

***Location/Storage:*** *Specify the location(s), including building and room numbers, where work will be performed within the export-controlled items and information and specifically where the items will be stored within the location****.***

|  |
| --- |
| Click or tap here to enter text. |

***Physical Marking:*** *Describe the markings or warnings that will be placed on export-controlled items and information or explain why they are not practical or possible.*

|  |
| --- |
| Click or tap here to enter text. |

***Security Measures:*** *Provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access (i.e. secure doors, limited access, time blocking, security badges)*

|  |
| --- |
| Click or tap here to enter text. |

|  |
| --- |
| Information Security Plan |

Appropriate measures must be taken to secure controlled electronic information, including User IDs, password controls, SSL, or other approved encryption technology. Coordinate with campus IT personnel, as needed.

***Location/Storage/Access:*** *List all IT resources (computers, servers, systems, etc.) that will be used to store or process the export-controlled information and all individuals with administrative access to IT resources who are not Project Personnel.*

|  |
| --- |
| Click or tap here to enter text. |

***Digital Marking:*** *Describe the markings or warnings that will be placed on export-controlled items and information, if applicable (i.e. watermarks, headers, footers)*

|  |
| --- |
| Click or tap here to enter text. |

***Security Measures:*** *Describe any project specific security methods or procedures that will be employed for data storage and transmission (i.e. user IDs, password protection, encryption)*

|  |
| --- |
| Click or tap here to enter text. |

|  |
| --- |
| Recordkeeping |

Current TCP documentation shall be maintained by both the Responsible Party and the Export Controls Office. The TCP must be maintained for as long as the covered items and information, identified in the TCP, require protection, and are maintained by SIU. This requirement applies regardless of funding status.

U.S. export control laws and regulations require that all records associated with export-controlled items, technology, software, technical data, and information must be retained. The PI and their Unit are responsible for maintaining the records in compliance with these federal laws and regulations, as well as SIU policy.

SIU’s policy is to maintain export-related records based on individual controlled items or activities. Unless otherwise provided for or instructed by the Office of the General Counsel, all records shall be maintained consistent with the SIU record retention policy, and shall be retained no less than 5 years after the TCP termination date or license termination date, whichever is later.

If ITAR-controlled technical data is exported under an exemption, certain records of the transaction must be kept even beyond SIU’s 5-year retention period (reference 22 CFR 122.5 and 123.26). Those records include:

* A description of the unclassified technical data
* The name of the recipient/end-user
* The date/time of export
* The method of transmission (e.g. email, fax, telephone, FedEx)
* The exemption under which the export took place

BIS has specific record-keeping requirements (reference 15 CFR 762.6). Generally, records required to be kept by EAR must be kept for a period of 5 years from the last export date. However, if BIS or any other government agency makes a request for such records following a voluntary self-disclosure, the records must be maintained until the agency concerned provides written authorization otherwise.

|  |
| --- |
| Self-Evaluation |

Self-evaluation is a critical component of SIU’s ongoing compliance monitoring. Self-evaluation is an internal assessment process in which procedures are reviewed and any findings reported to the project director or PI and the designated export control official. This review shall

include ensuring that all sections of the TCP are current. The PI/Responsible Person shall report on the findings of the self-evaluation to the Director of Export Controls.

***Self-Evaluation Schedule: It is recommended that the TCP be reviewed/evaluated at least once every year. Describe how often you plan to review/evaluate your TCP:***

|  |
| --- |
| Click or tap here to enter text. |

In the event that a violation or breach of one or more of the provisions contained within this TCP is suspected or known, the person with knowledge of such violation, breach or concern shall immediately report the matter to the PI/Responsible Person (who in turn shall report the matter to the Export Controls Office) or shall report the matter directly to the Export Controls Office.

|  |
| --- |
| Termination of Export-Controlled Activity/Project |

Upon completion of this project, all *export-controlled items and information* must be disposed of in accordance with applicable sponsor terms and U.S. export control requirements. It may be necessary to keep certain security measures in effect after the conclusion of a research activity to comply with export control laws and regulations and protect residual export-controlled technical data, information, or equipment.

The TCP can be closed if the export-controlled data or equipment has been returned to the sponsor, destroyed, or determined to be no longer export-controlled. However, all records and documents that pertain to export licenses and agreements related to controlled articles and technical must be retained in accordance with SIU policy and federal regulations.

***Destruction of Materials: How will export-controlled items or information be handled at the end of the research project (i.e. shredding, destroy hard drive, file wiping, return to sponsor)?***

|  |
| --- |
| Click or tap here to enter text. |

**Appendix A**

|  |
| --- |
| Unit/Export Control Approval and Responsible Person Certification |

Prior to Certification by the Responsible Person, both Unit Head and Export Controls Office approvals must be obtained.

***Unit Head Approval:***

|  |  |
| --- | --- |
| **Printed Name:** |  |
| **Signature:** |  |
| **Date:** |  |

***Export Controls Office Approval:***

|  |  |
| --- | --- |
| **Printed Name:** |  |
| **Signature:** |  |
| **Date:** |  |

By signing below, I certify that:

* The TCP has been approved by my Unit Head and the Export Controls Office.
* I have read and understand the terms and conditions of this TCP.
* All information found in this TCP is accurate and complete to the best of my knowledge.
* I am electing to participate in this project and understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export-controlled items, technology, software, technical data, or information to unauthorized persons.
* I have taken the required export control training.
* I agree to inform the SIU Export Controls Office immediately after I become aware of any changes to the information provided in, or affecting, this TCP.

***Responsible Person Certification:***

|  |  |
| --- | --- |
| **Printed Name:** |  |
| **Signature:** |  |
| **Date:** |  |

**Appendix B**

|  |
| --- |
| Participant Briefing and Certification |

**Participant Responsibilities:** Participants may be held personally liable for violations of the EAR and the ITAR, with significant financial and criminal penalties as a result. It is extremely important that participants exercise care and caution in using, disclosing, or transferring export-controlled information, items, technology, or software with others inside and outside the United States.

Export-controlled items and information cannot be transferred without prior authorization from the appropriate federal agency. Participants must clearly identify and secure access to export-controlled items and information to prevent unauthorized access or use. Participants must securely store export-controlled information in locked filing cabinets, locked drawers, or under password-protected computer files.

All project personnel must sign a TCP certification.

By signing below, I certify that:

* I have read and understand the terms and conditions of this TCP.
* I am electing to participate in this project and I understand that I could be held personally liable if I unlawfully allow access to or disclose, regardless of form or format, export-controlled information, items, technology, or software to unauthorized persons.
* I understand that the law makes no specific exceptions for non-U.S. students, visitors, or any other person not pre-authorized under a TCP to access export-controlled information, items, technology, or software.
* I have been briefed by the Principal Investigator/Responsible Person and that I agree to comply with the requirements in the TCP.
* I have taken the required export control training.
* I agree to immediately contact the Principal Investigator/Responsible Person with any questions I may have regarding the designation, protection, or use of export-controlled information, technology, software, or items.

***Responsible Person Certification:***

|  |  |
| --- | --- |
| **Printed Name:** |  |
| **Signature:** |  |
| **Date:** |  |

**Appendix C**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Additional Project Personnel | | | | |
| **#** | **Name** | **Country of Citizenship** | **Role Related to Controlled Item** | **Date Screening Cleared** |
| 1 | Enter text. | Enter text. | Enter text. | Select a date. |
| 2 | Enter text. | Enter text. | Enter text. | Select a date. |
| 3 | Enter text. | Enter text. | Enter text. | Select a date. |
| 4 | Enter text. | Enter text. | Enter text. | Select a date. |
| 5 | Enter text. | Enter text. | Enter text. | Select a date. |
| 6 | Enter text. | Enter text. | Enter text. | Select a date. |
| 8 | Enter text. | Enter text. | Enter text. | Select a date. |
| 9 | Enter text. | Enter text. | Enter text. | Select a date. |
| 10 | Enter text. | Enter text. | Enter text. | Select a date. |
| 11 | Enter text. | Enter text. | Enter text. | Select a date. |
| 12 | Enter text. | Enter text. | Enter text. | Select a date. |
| 13 | Enter text. | Enter text. | Enter text. | Select a date. |
| 14 | Enter text. | Enter text. | Enter text. | Select a date. |
| 15 | Enter text. | Enter text. | Enter text. | Select a date. |
| 16 | Enter text. | Enter text. | Enter text. | Select a date. |
| 17 | Enter text. | Enter text. | Enter text. | Select a date. |
| 18 | Enter text. | Enter text. | Enter text. | Select a date. |
| 19 | Enter text. | Enter text. | Enter text. | Select a date. |
| 20 | Enter text. | Enter text. | Enter text. | Select a date. |

**Appendix D**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Additional Export-Controlled Items and Information | | | | |
| **#** | **Name of Item or Information** | **Type** | **EAR or ITAR?** | **Classification\*** |
| 1 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 2 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 3 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 4 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 5 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 6 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 7 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 8 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 9 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 10 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 11 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 12 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 13 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 14 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 15 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 16 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 17 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 18 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 19 | Enter text. | Choose an item. | Choose an item. | Enter text. |
| 20 | Enter text. | Choose an item. | Choose an item. | Enter text. |

***\*Provide the applicable U.S. Munitions List category and subparagraph if subject to the ITAR or the Export Control Classification Number (ECCN) if subject to the EAR.***