**University of Wisconsin-Whitewater
Export Controls
Technology Control Plan**

|  |  |
| --- | --- |
| **UWW Grant #:** Click here to enter text.**Est. Date:** Click here to enter text. | **Sponsor:** Click here to enter text.**Sponsor Award #:**Click here to enter text. |
|  |  |

1. **Applicable ECCN or USML Category:** Click here to enter text.
2. **Description:**Click here to enter text.
3. **Departmental Responsibilities:**

It is the department’s responsibility to:

1. Provide a research area that will accommodate the electronic and physical information security plan as outlined in this TCP;
2. Disseminating information regarding the security required for this area/project to University faculty/staff that will have access to the secured area and receiving their acknowledgement on this document;
3. Ensure that ORSP is made aware and has properly vetted any foreign nationals before they are made a part of the research team or have access to secure information or materials;
4. Reporting any incidents of non-compliance with this TCP to the Office of Research and Sponsored Programs.

UW-Whitewater Office of Research and Sponsored Programs will assign an export compliance administrator to assist the Principal Investigator (PI) and researchers with complying with this Technology Control Plan (TCP). The export compliance administrator will screen faculty, staff, students, and contractors, who will work on the project against the Denied Party list, the Entity List, the Unverified List, the Specially Designated Nationals List, the Debarred List, the NSA Nonproliferation Sanctions List and General Order 3 to Part 736 of the EAR.

UWW Office of Research and Sponsored Programs, the export compliance administrator, UW System Auditors, or the Department Head will periodically evaluate compliance with this TCP. Any item of issue will be reported to the UWW Empowered Official.

1. **Physical Security and Personnel Access**
2. Identify the University Staff who will be working on or have access to this project

|  |  |  |
| --- | --- | --- |
| **Name** |  | **Nationality** |
| Click here to enter text. |  | Click here to enter text. |
| Click here to enter text. |  | Click here to enter text. |
| Click here to enter text. |  | Click here to enter text. |
| Click here to enter text. |  | Click here to enter text. |
| Click here to enter text. |  | Click here to enter text. |
| Click here to enter text. |  | Click here to enter text. |

***No additional personnel may be assigned to or have access to this project***

 ***without first notifying the Office of Research and Sponsored Programs.***

**5. Identifying Foreign Nationals as Personnel**

1. Are foreign nationals authorized to work on this project?
*(NOTE****:*** *Green Card Holders are considered U.S. Persons for purposes of export laws.)*

[ ]  Yes [ ]  No
2. If yes, is an export authorization required?

[ ]  Yes [ ]  No
3. If yes, has one been obtained?
*(NOTE: No foreign nationals may begin working on the project until such authorization is obtained and activated.)*
[ ]  Yes [ ]  No [ ]  N/A
4. What is the authorization number?: Click here to enter text.
5. What is the expiration date?: Click here to enter text.
6. Who is the UA holder?: Click here to enter text.
7. Email: Click here to enter text. Phone: Click here to enter text.
8. **Research Location and Security**

***NOTE:*** *Individuals with keys or key cards are expressly prohibited from permitting*

 *others to use their keys or key cards for access to the research site.*

 *Doors to secured areas may not be propped or left open.*

1. Where with the research take place?
Click here to enter text.
2. How will the room be secured?
Click here to enter text.
3. Who will have access to the keys or security code?
Click here to enter text.
4. If the room has multiple uses, how will the work areas be segregated to ensure there
 are no inadvertent transfers of project information or details?
Click here to enter text.

e) How will the project equipment be stored?
Click here to enter text.

f) How will controlled equipment be tagged or identified?
Click here to enter text.

g) **Meetings** - Attendance must be taken at all meetings and records kept of attendance and items discussed. Doors must be kept closed and all papers collected and white boards erased at meeting end.

h) **Visitors** - The researchers and staff who are authorized to enter the room when export controlled material is present will escort all visitors and keep visitor logs during the time export controlled material is in use. The departmental export control administrator must be contacted in advance of the visit to approve all visitors prior to granting access to the room and will document citizenship of all visitors when making access determinations.

i) **Facilities Management and Custodial Services** - The custodial and Facilities Management staff access must be coordinated with the researchers so that sensitive materials are securely locked away during their visits.

j) Are there any restrictions on public dissemination of project-related information (i.e.: publications or presentation) restrictions?

[ ]  Yes [ ]  No

k) If yes, is there an approved Waiver of Publication Rights in place?

 [ ]  Yes [ ]  No

If yes, please explain how this restriction will be managed:
Click here to enter text.

k) **Procurement** – Procurement of parts, tooling and equipment specifically designed, developed, configured, adapted, or modified for use with an ITAR-controlled item must be purchased by suppliers and vendors who can certify they are ITAR-compliant.

l) **Photography** - Non work-related photographs of export-controlled items are strictly prohibited. University Personnel listed in Section 4.a) above are the only individuals permitted to take photos. Photos must be stored in secure locations.

m) **Disposal of Equipment** - Disposal of test equipment, tooling and other materials must be coordinated with the departmental export compliance administrator prior to disposition.

1. **Computing and Information Security**

**Authorized project personnel should not share or discuss project-related**

**Information with any individual not authorized to participate in the project.**

1. How will project-related laboratory notebooks and any other hard copy

 materials be stored?
Click here to enter text.

1. Where will electronic data be stored and who will have access to the data?
Click here to enter text.

c) How will access to electronic data be restricted to only those individuals authorized to access the data?
Click here to enter text.

 d) How will the information/deliverable be transmitted to the sponsor?
Click here to enter text.

1. Who is the assigned IT person? (Must be a U.S. Citizen)

Click here to enter text.

***Note:*** *Location of permanent file storage must be secure UW-Whitewater Computer Network. Any files removed from this system by any media must be encrypted for field use, then resaved on the secure campus network and removed from transfer media. Virus protection software must be provided for these computers. If isolation is not possible, 128-bit or better encryption will be utilized to protect information.*

1. Removable hard drives may be used for data back-up with 128-bit or better encryption. When not in use, the back-up removable drives must be securely locked away in a Click here to enter text., and only Click here to enter text. will have keys.

***Note:*** *Any computer hard drives containing sensitive information will be formatted at the end of the contract plus overwritten three times with a DOD disk-wipe program.****SPECIAL NOTE REGARDING EMAIL -*** *Export-controlled information/deliverables should not be distributed or received utilizing email without encryption under any circumstances. Personal Web accounts (i.e.: Gmail, Hotmail) accounts and free cloud data storage sites (i.e.: Google Drive) are not secure and should never be used as a form of communication or transfer of export-controlled project data.*

**8. Research Team Administrative Responsibilities**

1. **Document Marking** - generated documents containing export-controlled technical data must be marked with one of the following legends:
2. *“This information is subject to the controls of [pick one: the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR)] and should not be distributed to non-U.S. persons or outside of the U.S. without prior permission of the U.S. State dept.”*
3. *“ITAR- [or EAR-] controlled – do not distribute to non-U.S. Persons.”*

b) **Clean Desk Policy** - A clean-desk policy is in effect. Hard copies of project-related information should be locked in a secured/locked location (secured drawer or cabinet) when not in use and at the end of every day.

c) **Disposal of Media** - Papers must be shredded (crosscut) not recycled. Disposal of computer floppy drives, compact discs, jump drives, and portable digital media devices that contain controlled technical materials must be coordinated with the departmental export compliance administrator or the MSU IT Security Officer.

 d) **Printers** - Any project information that is printed must be done on a printer located in one of the rooms listed in section 6. a) above. Printed information must be retrieved immediately.

1. **INTERNATIONAL TRAVEL**

1. Will there be any international travel associated with this project?

[ ]  Yes [ ]  No

If so, when and where, if known: Click here to enter text.

*Contact the ORSP as far in advance of the trip as possible (see special note below).*

Computers or other electronic storage devices containing restricted information should not normally be used for travel. If a computer is necessary for international travel, all unnecessary technical information not required for the trip should be removed and any information which is required must be authorized for the destination and end use.

For meetings, foreign travel, emails, symposiums, etc., where unlicensed controlled technology is potentially discussed, prior approval will be sought from **(sponsor)** and the **(government agency)** and licenses obtained if necessary.

***SPECIAL NOTE REGARDING REMOTE DATA ACCESS*** *– Reviewing export-controlled information on UW-Whitewater servers via remote desktop or VPN access is considered exportation of controlled information to the area where you are accessing the data. Traveling with export-controlled data on laptop hard drives and/or other media devices is also considered exportation. ORSP can work with you to obtain the necessary licenses for access to your data while traveling abroad, however this process can take months, be sure to contact us as soon as possible to discuss any potential travel.*

1. **RECORDKEEPING**

All records including technical data and records of export (both electronic and hardcopy information) must be kept for at least five (5) years minimum from the expiration of authorizations or date of last export. Copies of records must be given to the departmental export compliance administrator for archiving at the close of the project or upon termination of the agreement or personnel departure. Export controlled project data shall be stored for the required period in a secure network location managed by the Department Export Control Administrator in electronic format that cannot be altered (e.g. pdf) and permanently deleted from any storage media (computers, discs, thumb drives, other network locations, etc.).

 **11. COMMUNICATION PLAN**

All personnel authorized to work on this project will be briefed on this TCP, will receive a copy of it, and will sign for receipt and to acknowledge they have read it. Any new personnel assigned to this project must be briefed and sign an acknowledgment prior to beginning their assignment.

Employees will receive refresher training on this TCP at least once annually. Employees should also review the UWW website [http://www.uww.edu/orsp](http://www.uww.edu/orsp/compliance/export%20controls) Research Compliance, Export Controls for more information.

A copy of this TCP should be sent to your Department Head and to the Office of Research and Sponsored Programs.

**Briefing Form Acknowledgement**

I acknowledge by signing below that I have been briefed on and received a copy of the content of the Technology Control Plan for the project listed below.

|  |  |
| --- | --- |
| **UWW Grant #:** Click here to enter text.**Est. Date:** Click here to enter text. | **Sponsor:** Click here to enter text.**Sponsor Award #:**Click here to enter text. |
|  |  |

I certify that I will follow the safe guards set-forth for the protection o

***Form must be signed by all investigators***

|  |  |  |
| --- | --- | --- |
| **Printed Name** | **Signature** | **Date** |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |
| Click here to enter text. |  |  |