**Technology Control Plan**

|  |  |
| --- | --- |
| **Principal Investigator/Supervisor:**  | **Department:**  |
| **Laboratory:**       | **Location:**       |
| **Project Name(s)/Identification:**       |
| **Project Description:** |

Please note that Appendixes A and B can be found at https://research.wisc.edu/kb-article/?id=35042

Please note that capitalized terms are defined in Appendix B.

Export Controlled Material can include any of the following: physical items, technology, data, software, documents, pictures, blueprints and schematics

1.0 Monitoring

1.1 Personnel shall safeguard Export Controlled Material from unauthorized use and disclosure by following the rules in this TCP.

1.2 Foreign Entities shall not be given access to any Export Controlled Material or participate in any project or research that contains Export Controlled Material unless that person has received the appropriate license allowing access to the information or has been cleared by the Export Control Office.

1.3 If Export Controlled Material is discovered to be missing, the UW Police must be informed as soon as possible, not more than 12 hours after discovery. The Export Control Office must also be contacted within one business day of the time in which the Material is discovered missing.

1.4. If the PI leaves their current position at the UW or the UW entirely, they must contact the Export Control Office PIROR to leaving so all Export Controlled Material can be accounted for.

2.0 Physical Security

2.1 All Export Controlled Material, including physical items, software, data etc., must be kept in secure room(s) which can be locked and have access limited only to those people who are directly involved in the project(s) being carried out and authorized to be in said rooms.

2.1.1 An alternative to a secure room is a lockable file cabinet or other receptacle as long as the Export Controlled Material is of a size that may reasonably fit in said cabinet or other receptacle.

2.1.2 The room(s) and/or file cabinet, etc. in which the Export Controlled Material is used must not be generally accessible to department personnel but, rather, must have some measure in place to ensure that only those with authorized access may be allowed to enter. For example, it is not enough to have a lock on a room with Export Controlled Material inside if it is a general department lock where anyone who works in the department has a key. The room(s) must ONLY be accessible by individuals working on projects that are housed in that room.

 2.1.2.1. There may be a “department key” kept with the administration of the department to ensure access to the room in case of emergencies.

 2.1.3 Persons with access to these room(s) and/or file cabinet, etc. are prohibited from admitting anyone not authorized to have access to the secure room.

 2.1.4. If possible, the Export Controlled Material must be locked away and not generally accessible when not in use.

2.2 People with access to the Export Controlled Materials are prohibited from allowing access of those materials to anyone else who is not authorized to have access to the Export Controlled Material.

2.3 A list of personnel who are cleared to look at and/or use the Export Controlled Material will be kept and provided by the Principal Investigator and Project Manager of a particular project to the Export Control Office on request.

2.4 Visitors to areas that may contain Export Controlled Material shall be escorted at all times and shall not be given keys, passcards, ids, passwords, combinations or anything else that would allow entry or access to export controlled information.

 2.4.1. If these visitors will have unsupervised access to Export Controlled Material, it must be cleared with the Export Control Office in advance.

2.5 Export Controlled Materials must be shielded from the view of non-authorized personnel when are in proximity to Export Controlled Materials that would reveal information if merely viewed. This would include things like data, documents, and blueprints, but would not normally extend to merely viewing a piece of controlled technology.

2.6 Custodial, maintenance, technical and any other staff that require access to an area that contains Export Controlled Material for purposes of cleaning, maintenance, upkeep, or repair must be coordinated by the Project Manager, Principal Investigator and/or supervisor to ensure that all Export Controlled Material is secured and not accessible during the staff’s time in the area.

2.7 Conversations about Export Controlled Material may only take place in a secure location, such as a room with a closed door. They may not be held in public places where any Foreign Persons may be.

 2.8 All work done to build Export Controlled Materials in the Engineering Clean room and any other fabrication or equipment lab must follow all necessary security measures to ensure there is not a violation.

 2.8.1 While working on building, testing, maintaining etc. equipment in the Engineering Clean Room, only persons who are directly involved with the project may work on it.

 2.8.2 Persons directly involved with the project may not allow those not involved to work with, utilize, inspect etc. the Export Controlled Materials.

 2.8.3 When not working on the project, the Export Controlled Material must be locked away.

3.0 Physical Documents

3.1 Any physical documents, printed and/or photocopied, that contain Export Controlled Material must include the following warning:

**“This document contains data subject to export control regulations under United States law. Only authorized persons are allowed access to this data. Failure to comply with these laws may result in criminal and civil penalties. Please contact the Export Control Office for more information.”**

3.2 All physical documents that contain Export Controlled Material, when not in active use, must be kept in a locked file cabinet(s) or other lockable receptacle.

3.2.1. Documents may not be outside the locked file cabinet(s) or lockable receptacles when no authorized personnel are in the room, no matter how short their time away is.

3.2.2 Only those personnel directly involved with the project may have access to the file cabinet(s) or lockable receptacle.

3.2.3 Individuals with access to the file cabinet(s) or lockable receptacle are prohibited from allowing access to a person not authorized to view the Export Controlled Material.

3.3 Documents containing Export Controlled Material must not be left in open view of anyone who is not authorized to view said documents.

3.4 Pictures of Export Controlled Material are not allowed unless prior authorization from a supervisor is given.

3.4.1 These pictures must not be mailed, faxed, e-mailed or any way transmitted to Foreign Persons or Entities without an export control license specifically allowing the Foreign Person or Entity access to that information.

3.5 Documents must not be taken out of the secure location to be viewed in a public space where non-authorized personnel may be able to view these documents.

3.5.1 **Please note,** it is not enough that non-authorized personnel did not view said documents, it is a violation of this agreement if documents are in a public space where they MAY be viewed by non-authorized personnel.

4.0 Computers and Laptops

4.1 Computers (including laptops, workstations, tablets etc.) that contain the Export Controlled Material must run an operating system with the latest security services and patches as well as firewall projection, antivirus software, and any other precautions that may be deemed necessary by an IT professional of the University.

 4.1.1 If needed, the Export Control Office will work with the PI to determine if additional security measures are needed for the current systems in use.

4.2 Computers that contain the Export Controlled Material will be accessible only with a unique userid and password.

4.2.1 Userids and passwords will only be issued to personnel who are directly working with the Export Controlled Data.

4.2.2 Personnel will not share their userids and/or passwords with anyone else.

4.2.3 Personnel will not log in using their userids and passwords and allow another person to work on that computer.

4.3 Personnel must lock, log off or shut down computers when not actively using them.

4.4 Computers that contain Export Controlled Material must be locked, logged off or shut down when not in direct line of sight of the person who has used their userid and password to log on.

4.5 Laptop computers that contain Export Controlled Material must not be left unattended under any circumstances and must be locked securely away when not in use.

4.6 Export Controlled Material on all computers shall be encrypted when not in active use.

 4.6.1. The Export Control Office will work with the PI or delegate to help to determine the correct level of encryption needed if requested.

4.7 If removable hard drives are used to backup data they must be securely locked away when not in use.

4.8 Export Controlled Material may not be stored on general cloud servers. The data may only be stored on UW-Madison servers.

4.8.1 Non-UW-Madison servers that store data may be approved once security measures are confirmed by an Information Technology professional and confirmed by the Export Control Office.

4.9 Other Technical Devices that can access Export Controlled Information including tablets, phones, etc. will maintain all security protocols that desktop and laptop computers normally have including, but not limited to, password protection, personal firewall, and restricted network usage.

4.9.1 Other Technical Devices that contain Export Controlled Material must be kept in a authorized individuals direct control or be securely locked away at all times.

4.9.2 The Export Control Office discourages loading, saving, viewing etc. Export Controlled Material on Other Technical Devices and Data Storage Devices.

4.10 Export Controlled Material in the form of software must only be accessible on computers, laptops etc. that are only accessible to those who are authorized to view the Export Controlled Information.

4.10.1 This software must never be loaded onto public computers or utilized on open networks.

 4.11 Export Controlled Material should not be loaded onto flash drives unless first cleared with the Export Control Office.

5.0 Transmission of Export Controlled Material

Please note: This includes electronic data.

5.1 Export Controlled Material may not be e-mailed to individuals who are not authorized to have access to said data.

5.2 Export Controlled Material may not be e-mailed to non-secure accounts such as yahoo, gmail, hotmail, etc. It may be e-mailed to Wisc Mail accounts.

5.3. Export Controlled Material may be uploaded to a UW-Box account with access given to individuals who are authorized to view said Export Controlled Material. It may not be uploaded to other drop box accounts.

5.4 E-mails containing Export Controlled Material may only be sent if encrypted by the originator.

5.4.1 The key code for the encrypted data must not be e-mailed. It must be transmitted over the phone by voice or fax.

5.5 Export Controlled Material may not be accessed through an unsecure wireless network.

5.5.1 If utilizing a wireless network to view Export Controlled Material, the network must be password protected.

 5.5.1.1. It is preferred that this network only be accessible to those who have access to the Export Controlled Material.

6.0 Travel

6.1 If an individual travels overseas, they may not take Export Controlled Material or work on said information while out of the country unless they first contact the Export Control Office to determine if a license is required.

6.2 Individuals may not access any Wisc Mail accounts that regularly receive Export Controlled Material while out of the country. Individuals must use a different e-mail address that does not receive e-mails regarding Export Controlled Material while traveling abroad to ensure that no Export Controlled Material is accessible by foreign servers.

6.3 Export Controlled Material shall not be taken for trips, meetings, symposiums, travel within the United States etc. on a Data Storage Device (i.e. flash drive, thumb drive, floppy disk, CD-ROMs) except when:

 The Data Storage Device requires a password to access it,

And

 The Data Storage Device is kept upon the person at all times or securely locked away when not on the person,

And

The data contained on the hardware is encrypted.

 6.3.1. Please note, you may not leave any of these Data Storage Devices in your hotel room unless they are locked in a safe in the room. Simply leaving them in a locked hotel room does not constitute sufficient security.

6.4 Export Controlled Material on Data Storage Devices should not be taken out of the country without a license. If Export Controlled Data is taken out of the United States in/on a Data Storage Device it is considered exported.

6.5 The Export Control Office recommends not taking any computer, laptop, or other technological device containing export controlled data out of the United States. **There is a high likelihood that all information on your laptop will be copied to a foreign system when travelling outside the country.**

6.5.1 If travelling outside the United States with a computer that contains Export Controlled Material, the data must be encrypted and must not be accessed while outside the country for any reason.

6.5.2. All electronics including computers, tablets, flash drives etc. must be under the effective control of the traveler at all times.

6.6 The Export Control Office recommends travelers utilize DoIT’s checkout program to obtain technology when traveling abroad to lessen the possibility of compromising data. More information can be found at <https://it.wisc.edu/guides/the-academic-professionals-guide-to-safe-computing-when-traveling-abroad/>. Information on checkout can be found at https://it.wisc.edu/services/equipment-checkout/.

7.0 Shipping

 7.1 Shipping of Export Control Materials needs to be discussed and cleared with the Export Control Office *prior* to shipment.

7.2 No employee of UW-Madison acting on their own or on another’s behalf will, without approval by the Export Control Office, transmit, ship, hand carry or in any way send Export Controlled Materials including data or direct someone to do so on their behalf to a Foreign Entity.

8.0 Disposal

8.1 All physical documents and their copies (including photographs) containing Export Controlled Material must be destroyed by shredding so all information contained therein is indistinguishable.

8.2 When the project is finished and a PI no longer wants to maintain security measures for any Export Controlled Material that is in electronic form, the material must be deleted.

8.2.1 Any computer hard drive containing Export Controlled Material will be scrubbed and reformatted and overwritten three times with a DOD disk-wipe program.

8.2.2 Please contact the Export Control Office at the conclusion of a project for specific guidance.

8.3 Any Export Controlled Materials must be destroyed or securely stored so it cannot be accessed by unauthorized personnel at the completion of a project.

 8.3.1 If sending Export Controlled Material to SWAP, please contact the Export Control Office.

9.0 Training

9.1 All persons with access to a project that utilizes Export Controlled Material will sign a document acknowledging receipt and understanding of this TCP (see Attachment A).

9.2 After an export control project has been authorized but before work begins, all personnel involved must take training to ensure compliance with the TCP.

 9.2.1. Meeting with the PI and/or the Export Control Office to ensure that the TCP is understood is sufficient training.

9.3 All those involved with this project must sign the agreement in Attachment A not to transfer, transmit, or in any way give Export Controlled Material to unauthorized foreign persons.

10.0 Termination

10.1 At the termination of a project or of a specific person from a project that uses Export Controlled Material, that person must turn in all badges, keys, key cards etc. to the supervisor of the project within 24 hours of the termination to ensure the security of the data.

10.2 At the termination of a project or a specific person from a project that uses Export Controlled Material, user names and passwords must be locked out from having access to the Export Controlled Material within 24 hours of termination.

11.0 Responsibilities

11.1 Any person who has knowledge of a potential violation of the TCP or any applicable export control laws must contact the Export Control Office as quickly as possible(no more than three(3) business days). Contacts can be found at the end of this Technology Control Plan.

11.2 The Principal Investigator and supervisor on a specific project will be responsible for implementing all necessary security measures to ensure that all Export Controlled Material is secure per this Technology Control Plan.

11.2.2 If a Principal Investigator has any question regarding the necessity of licenses or any security measures they must contact the Export Control Office for guidance.

11.3 The Principal Investigator must notify the Export Control Office if any of the following occur:

11.3.1 Any foreign nationals are added to the list of those who require access to the Export Controlled Material.

11.3.2 The scope of the project changes.

11.3.3 Acquisition of new equipment, software or technology for the project.

11.4 Export Controlled Material may only be used for the purpose of performing the research or services outlined in contracts received through UW-Madison. It may not be used for any extraneous projects or for personal, financial, commercial or political gain.

12.0 Contacts

 12.1 Tom Demke

 Export Control Officer

 Atmospheric, Oceanic & Space Sciences

 1225 W. Dayton St

 Madison, WI 53706

 Tom.demke@ssec.wisc.edu

 608-262-8659

 12.2 Bethany Nelson

 Export Control Coordinator

 Atmospheric, Oceanic & Space Sciences

 1225 W. Dayton St

 Madison, WI 53706

 Bcnelson2@wisc.edu

 608-261-1128

**Attachment A**

**Acknowledgement of Technology Control Plan**

I,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (**print name**),will be working on an Export Controlled Project with Prof\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(**Professor**) and acknowledge that I have received and understand the Technology Control Plan. I agree to comply with all of its requirements. I also agree that I will not transfer, transmit, give, import or in any way disclose Export Controlled Material that I have interaction with in the course of this project to any individuals not authorized to view it (including foreign persons who have not received prior authorization to interact with said data). I will inform my PI/Supervisor of any violations of this TCP as soon as possible after discovery.

Signature: Witnessed By Supervisor:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Print name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-Mail:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ E-Mail:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telephone #:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Telephone #:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

At the start of a project, this form should be signed by all individuals involved and copies sent to the export control office.

This form will be retained by the supervisor or project investigator as retention records require.