**Wright State University Technology Control Plan Briefing for Export-Controlled Technology and Information**

Prior to the acceptance or initiation of any sponsored research project that involves the use, receipt or development of export-controlled technology, technical data or other restricted information or materials, Wright State University’s Export Control Office requires that the faculty or staff member that acts as the principal investigator for the research develop a plan for the safe and lawful management of the project’s controlled elements prior to acceptance of the award and commencement of the research.

The research project identified below may involve the receipt, use and/or development of technical data that is controlled under United States export control laws: the Export Administration Act and Export Administration Regulations (“EAR”), enforced by the Bureau of Industry and Security in the Department of Commerce, or the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations (“ITAR”), enforced by the Directorate of Defense Trade Controls in the State Department. Links to information about the ITAR and EAR may be found at Wright State’s Export Controls website at <http://www.wright.edu/rsp/Security/export_controls.htm>

Since this project has been identified as having export control restrictions, technical information, data, materials, software, hardware, and any other controlled items or elements must be secured from use, access, and possible observation by unlicensed foreign nationals. Security measures will be appropriate to the classification involved and will be disclosed through the completion of the Technology Control Plan documentation and certification of that plan. It is the responsibility of the Principal Investigator (PI) to develop a written TCP which must be approved and signed by the University’s Export Control Administrator.

The Principal Investigator must ensure each eligible person working on the project has read and understands the information presented in this briefing and the TCP, and that no ineligible persons have access. In addition, the Export Control Administrator may meet with project personnel regarding the handling of Export‐Controlled Technology/Information and the Technology Control Plan. Project personnel must sign the TCP Certification before they can begin work on the project. The signed TCP and TCP Certification should be returned to Ellen Reinsch Friese in Research and Sponsored Programs at 201J University Hall. Copies of the signed TCP and TCP Certification will be sent to the PI and the Director, Pre-Award in the Research & Sponsored Programs office.

**TECHNOLOGY CONTROL PLAN**

In accordance with export control regulations as specified in EAR and ITAR, a Technology Control Plan is required for this project in order to prevent unauthorized export of controlled technology or information deemed to be sensitive to national security or economic interests. This form contains the basic and minimum elements of the TCP.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date: |  | | Title of Sponsored Project/Activity: | |  | | | |
| Technical description of item/technology/  equipment/software to be controlled: | | | | |  | | | |
| Responsible Individual/  Principal Investigator: | | | |  | | | Department & Address: |  |
| Phone: | |  | | | | E-mail: |  | |

1. **Physical Security Plan:** *(Project data and/or materials must be physically protected from observation or access by unauthorized individuals by performing project activities in secured research locations, or during secure time blocks when observation by unauthorized persons is prevented and other information and technology security measures are implemented to ensure unauthorized access.)*
   1. **Location:** *(describe the physical location of EACH sensitive technology/item using building and room numbers. A schematic of the immediate location is highly recommended to be attached as an Appendix to this plan.)*
   2. **Physical Security:** *(provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access, i.e., secure doors, limited access, security badges, etc.)*
   3. **Perimeter Security Provisions:** *(describe perimeter security features of the location of the protected technology/item)*
2. **Information Security Plan:** *(Appropriate measures should be taken to secure controlled electronic information, including User ID’s, password control, SSL or other approved encryption technology. Database access must be managed via a Virtual Private Network (VPN), allowing only authorized persons to access and transmit data over the internet, using 128-bit SSL or other advanced, federally approved encryption technology.)*
   1. **Structure of IT security:** *(describe the information technology (IT) setup/system at each technology/item location)*
   2. **IT Security Plan:** *(describe in detail your security plan, i.e., password access, firewall protection plans, encryption, etc.)*
   3. **Verification of Technology/Item Authorization:** *(describe how you are going to manage security on export controlled technology in case of termination of employees, individuals working on new projects, etc.)*
   4. **Conversation Security:** *(describe your plan for protecting information about controlled technology in conversations. Discussions about the project or work product are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party subcontractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.)*
3. **Item Security**
   1. **Item Storage:** *(describe your plan for protecting the physical technology and/or by-product. Both soft- and hard- copy data, notebooks, reports and research materials must be stored in locked cabinets; preferably in rooms with key-controlled or badge-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing “export controlled” technology are to be physically secured from unauthorized access as well.)*
4. **Project Personnel**
   1. Clearly identify every person (including their national citizenship) who is determined to have authorized access to the controlled technology:

|  |  |
| --- | --- |
| **Full Name** | **Country of Citizenship** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. **Personnel Screening Procedures:**
   1. At a minimum, you must review entities and denied parties list found on the Department of Commerce website at: <http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm>. Controlled technology cannot be shared with any person or entity found on any of these lists. Describe any other screening procedures (i.e., criminal, driver’s license, etc.):
2. **Training/Awareness Program**
   1. Describe how you will inform U.S. employees and/or foreign nationals about restrictions and security measures for this program regarding the controlled technology:
3. **Self Evaluation Program**
   1. Self Evaluation Schedule: (describe how often you plan to review/evaluate your TCP. Plans must be re-evaluated annually.)
   2. Action Item and Corrective Procedures: (describe your process to address findings in your self evaluation audits)
4. **Acknowledgements:**

**Principal Investigator: Department Head:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Signature | Date |  | Signature | Date |
|  | |  |  | |
| Printed Name | |  | Printed Name | |
|  |  |  |  |  |
| **Associate Vice President for RSP:** | |  | **TCP Review:** | |
|  |  |  |  |  |
|  |  |  |  |  |
| Signature | Date |  | Signature | Date |
| Ellen Reinsch Friese | |  |  | |
| Printed Name | |  | Printed Name | |

**TECHNOLOGY CONTROL PLAN CERTIFICATION**

|  |  |
| --- | --- |
| Principal Investigator/ Responsible Party: |  |
| Department: |  |
| Sponsor Name: |  |
| Project Title: |  |

This is to acknowledge I have read and understand the “Briefing on the Handling of Export-Controlled Information”, and that I agree to comply with the requirements of the Technology Control Plan (TCP).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Signature | Date |  | Signature | Date |
|  | |  |  | |
| Printed Name/Role | |  | Printed Name/Role | |
|  |  |  |  |  |
|  |  |  |  |  |
| Signature | Date |  | Signature | Date |
|  | |  |  | |
| Printed Name/Role | |  | Printed Name/Role | |
|  |  |  |  |  |
|  |  |  |  |  |
| Signature | Date |  | Signature | Date |
|  | |  |  | |
| Printed Name/Role | |  | Printed Name/Role | |
|  |  |  |  |  |
|  |  |  |  |  |
| Signature | Date |  | Signature | Date |
|  | |  |  | |
| Printed Name/Role | |  | Printed Name/Role | |
|  |  |  |  |  |

Acknowledgement of Immediate Supervisor:

|  |  |
| --- | --- |
| Signature | Date |
|  | |
| Printed Name/Role | |
|  |  |

*Signed TCP Certification must be returned to Ellen Reinsch Friese, Associate Vice President for Research,*

*Sponsored Research and Programs, 201J University Hall, 3640 Colonel Glenn Highway, Dayton, Ohio 45435-0001.*

TCP Program Reviewed and Certification Received:

|  |  |
| --- | --- |
| Signature | Date |
|  | |
| Printed Name/Role | |