**Briefing on the Handling of Export Controlled Technology/Information**

This project has been identified as involving or potentially involving technology/information that is export-controlled under either the State Department’s International Traffic in Arms Regulations (ITAR) or the Departments of Commerce’s Export Administration Regulations (EAR). Links to information about ITAR and EAR can be found on the University Research Services website at: <https://research.okstate.edu/faculty-resources/export-control.html>.

In summary, export-controlled technology/information means activities, items, and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application. Typically, this does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain.

It is unlawful under the ITAR and EAR to send or take export-controlled technology/information out of the U.S.; disclose orally or visually, or transfer export-controlled technology/information to a FOREIGN PERSON inside or outside the U.S. without proper authorization. A license may be required for foreign nationals to access export-controlled technology/information. A foreign national is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

Since this project has been identified, technical information, data, materials, software, or hardware, i.e.; technology generated from this project/activity, 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 **Technology Control Plan** (TCP) which must be approved and signed by Ron Van Den Bussche, Senior Associate Vice President, Division of the VP for Research. The PI must ensure each person working on the project has read and understands the information presented in this briefing and the TCP. In addition, Ron Van Den Bussche may meet with project personnel regarding the handling of Export-Controlled Technology/Information and the TCP. Project personnel must sign the **TCP Certification** before they can begin work on the project. The signed **Technology Control Plan** and **TCP Certification** should be returned to Ron Van Den Bussche, ron.van\_den\_bussche@okstate.edu. Copies of the signed TCP and TCP Certification will be sent to the PI and Sponsored Programs staff member.

**TECHNOLOGY CONTROL PLAN**

In accordance with export control regulations as specified in EAR and ITAR, a Technology Control Plan is required for this project to prevent unauthorized export of controlled technology 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 shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of “work-in-progress”)*
	1. **Location:** *(describe the physical location of EACH sensitive technology/item to include building and room numbers. A schematic of the immediate location is highly recommended)*
		*
		* **Term of Use**: *(Indicate the length of time the identified space will be used or controlled for this project.)*

* 1. **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.)*
		+
	2. **Perimeter Security Provisions:** *(describe perimeter security features of the location the protected technology/item)*
		+
1. **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.)*
		*
2. **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 are stored in locked cabinets; preferably in rooms with key-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)*
		*
3. **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 (to include item b. Suspicious Contacts):
		*
	2. Suspicious Contact Reporting:
	Unsolicited contact from unknown individual(s) or entities asking for project specific information, or phishing for journal reviews, or general information that doesn’t seem to fit background. Contact can be from e-mails, phone, or personal interaction. Any suspicious contact should be reported to Dr. Ron Van Den Bussche, ron.van\_den\_bussche@okstate.edu or 744-6501.
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 Dean for Research:** |  | **TCP Review:** |
|  |  |  |  |  |
|  |  |  |  |  |
| Signature | Date |  | Signature | Date |
|       |  | Ronald Van Den Bussche |
| 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 Technology/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 Ron Van Den Bussche, Senior Associate Vice President,
Division of the VP for Research. Contact: 405-744-6501 or* *ron.van\_den\_bussche@okstate.edu**.*

TCP Program Reviewed and Certification Received:

|  |  |
| --- | --- |
| Signature | Date |
| Ron Van Den Bussche |
| OSU Senior Associate Vice President |