

**TECHNOLOGY CONTROL PLAN (TCP)
FOR EXPORT CONTROLLED TECHNOLOGIES**

The University of Toledo is committed to export control compliance. The purpose of the Technology Control Plan (TCP) is to ensure that technical information and/or technical data which is not specifically exempted as Fundamental Research and/or Educational Information by EAR or ITAR is not transferred to Foreign Persons (including employees, visitors, or students) unless approved by license or other authorization with the Department of State, Office of Defense Trade Controls (ODTC) or Department of Commerce. The Principal Investigator (PI), with assistance from the Research and Sponsored Programs (RSP) office, is responsible for the development and implementation of the Technology Control Plan. Questions regarding this plan may be directed to Gary Rafe, Ph.D., Export Control Compliance Analyst at 419.530.2227.

***Complete and sign this form and return it to the Office of Research and Sponsored Programs.***

1. **PROJECT IDENTIFICATION**

**Project Title**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Date**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Sponsor**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Principal Investigator**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Signature:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Export Control Officer or Empowered Official:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **PROJECT DESCRIPTION**

(*Please provide background and descriptions of the use of export controlled items, technology and information. Include ECCN or ITAR USML list designations if known.*.)

1. **PERSONNEL ACCESS**

**Personnel:**

(*Identify every person, together with citizenship or immigration status, who is to have access to export-controlled materials*.)

**Screening:**

(*Describe any information on the type of background check and any additional required reviews that will be employed beyond the University’s standard background check procedures for all employees*.)

1. **PHYSICAL SECURITY**

**Location:**

(*Describe the physical location of each sensitive technology/item: building and room*.)

**Item Marking:**

(*Export-controlled materials must be clearly identified and marked as such*.)

**Physical Security Measures:**

(*Describe how equipment, technology, data and other controlled information will be shielded from unauthorized persons including descriptions of relevant security systems such as badges, escorts, visitor logs and other types of building access restrictions*.)

1. **INFORMATION SECURITY**

 **IT Security Plan:**

(*Describe the information technology security for data and other export-controlled information*.)

 **Transmission Protocols:**

(*Describe whether export-controlled information will be transmitted electronically or physically, and the protocols for secure transmission*.)

**Conversation Security:**

(*Describe protections from employee transfer to unauthorized persons by conversation with unauthorized persons, such as confidentiality agreements, disclosure forms, exit procedures when persons leave the project, agreements with external collaborators*.)

1. **TRAINING AND AWARENESS**

All personnel with access to controlled information on this project must read and sign the Acknowledgement of Briefing and Handling of Export Controlled Information form. Additional information may be obtained by visiting the UToledo Export Control web site ([http://utoledo.edu/research/ exportcontrol](http://utoledo.edu/research/%20exportcontrol) ). Additional export control training for this project may be conducted by the Export Control officer by contacting the RSP office (419-530-2844).

1. **PROJECT TERMINATION**

Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminate when the information has been destroyed or determined to be no longer export-controlled.

1. **COMPLIANCE ASSESSMENT**

As a critical component of the University’s ongoing compliance monitoring, self-assessment should be performed periodically and any relevant findings reported to the Export Controls Officer or the Empowered Official. The Export Control Compliance Analyst may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the Export Control Compliance Analyst or the Empowered Official for Export Controls.