**THE UNIVERSITY OF ALABAMA IN HUNTSVILLE**

**OFFICE OF RESEARCH SECURITY (ORS)**

**TECHNOLOGY CONTROL PLAN (TCP)**

**TCP-EC-2025-?? (Provided by ORS)**

**DATE**

**1) COMMITTMENT**

The University of Alabama in Huntsville (UAH) is committed to export controls compliance. A Technology Control Plan (TCP) is required to prevent unauthorized export or transfer of controlled items, materials, information, or technology. This document serves as a basic template for the minimum elements of a TCP and the safeguard mechanisms that need to be put into place to protect authorized access or use. Security measures and safeguards shall be appropriate to the export classification involved. Assistance with this form is provided by the Office of Research Security (ORS), Denise K. Spiller, Director, Export Control Compliance Officer, Janine Wilson, Assistant Director, Export Control Compliance Officer.

The individual(s) responsible for and committed to ensuring compliance with this (Names of PI and Co-PI).

# DESCRIPTION OF THE PROJECT/ACTIVITY INVOLVES OR HAS THE POTENTIAL TO INVOLVE SENSITIVE INFORMATION

All activities subject to Export Control Regulations and/or ITAR will remain out of view to Foreign Nationals (FN). ***Foreign Nationals (FN) are not allowed to be present in the same room or rooms as the Export Control Regulations and/or CUI, ITAR activities.***

**All individuals supporting this work will be** educated or briefed on the handling and protecting of Export Controlled Information, Controlled Unclassified Information (CUI), proprietary information, data, hardware or software.

**3) PHYSICAL SECURITY – (should include Physical Security Plan, Physical Security and Item Storage)**

ITAR and CUI documents will be stored electronically. Electronic files are stored on hardware encrypted USB drives which are stored in locked cabinets or safes in locked offices. Only project personnel will be allowed access to the ITAR and CUI documents. Accessing ITAR and CUI documents will be restricted to isolated computers in the Nonlinear and Complex Systems Laboratory provided by the UAH ORS Security Administrator or on encrypted computers approved for such use by the UAH ORS Security Administrator.

**4) INFORMATION SECURITY**

The University of Alabama in Huntsville (UAH) rules require all faculty, staff and students to ensure that sensitive digital research data is appropriately protected. In accordance with those rules, The University of Alabama in Huntsville will provide guidance on procedures for Protecting Sensitive Digital Research Data that will be followed for the protection of controlled and sensitive information under this TCP. Controlled data are categorized under the Data Classification Standard as Category I data.

The computers on and off campus are connected to the UAH internet. All project data and other related digital materials will be strongly password-protected. After sensitive data are generated on UAH computers, the data will be transferred off the computers using procedures described in the “Item Storage” section.

**5) PERSONNEL SCREENING**

All U.S. personnel with access to the controlled technology and their nationality are listed on the TCP Certification Form. Citizenship has been verified through the appropriate channels with Office of Research Security. ***All Foreign Nationals (FN) listed on the Certification Form will have access to unclassified information but not the controlled technology.***

**6) TRAINING AND AWARENESS**

All personnel with access to controlled information on this project will have completed the on-line Export Control Certification Web Training and Controlled Unclassified Information (CUI) Web Training. Additional training for this project may be conducted by the Office of Research Security (ORS). Annual Export Control and CUI training will be required for all personnel with access to the controlled information on this project.

**7) COMPLIANCE ASSESSMENT**

As a critical component to the University’s ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the Export Controls Officer at denise.spiller@uah.edu (256-824-6444) or to Janine Wilson at janine.wilson@uah.edu (256-824-3025). The Export Controls Officer 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 Officer.**

**8) CONTROLLED UNCLASSIFIED INFORMATION (CUI) HANDLING (This project currently does NOT contain CUI information; if that changes at any time during the duration of the project the PI will notify ORS immediately)**

# If this project contains CUI information the following will be strictly followed:

# All people with access to the CUI information will be properly trained on the handling of CUI information.

* All CUI information will be transmitted, processed and stored on UAH CUI approved systems only. All UAH CUI approved systems must be authorized by the UAH ISSM.

**9) ACCESS TERMINATION**

Security measures, as deemed appropriate, will remain in effect until the individual no longer requires access. When an individual no longer is working on the project the PI will notify ORS immediately.

**10) PROJECT TERMINATION**

Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect all sensitive information unless earlier terminated when the information has been destroyed or determined to be no longer export-controlled and/or controlled unclassified information. When computers reach its usable life, the hard drive will be forensically erased or destroyed using UAH hard drive destruction services provided by the Office of Research Security.