THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
OFFICE OF RESEARCH SECURITY
TECHNOLOGY CONTROL PLAN (TCP)

Individual Requesting and Responsible for TCP: Dr. xxxxxxx

Telephone Number: 256-961-xxxx

E-mail Address:

Request Date: 9/22/2016

Description of Controls (EAR/ITAR Category) Location(s) Covered by TCP
Building **Room(s)**

Project Personnel

List of Name(s)	**Citizenship**	**Export Training Date:**	**Signature:**
Jane Doe	**US**	**2/22/2017**	**XXXXXXX**

Is sponsored research involved? YES OR NO

Is a non-disclosure agreement involved? YES OR NO

Attachments:
1. TCP

Approved By:

_____ _____
Denise K. Spiller Date
Director Office Research Security
Export Controls Officer

TECHNOLOGY CONTROL PLAN (TCP)

1) COMMITTMENT

The University of Alabama in Huntsville (UAH) is committed to export controls compliance. The Office of Research Security (ORS) is responsible for implementation of technology control plans as applicable. Denise K. Spiller, Research Security Administrator; Export Control Compliance Officer is the main contact for export control issues. The individual responsible for and committed to ensuring compliance with this TCP is XXXXX

2) BACKGROUND AND DESCRIPTION OF THE USE OF SENSITIVE ITEMS AND INFORMATION

The one or more graduate students, who are approved will work on both of these projects, the projects will involve proprietary and export control activities SAMPLE

Activities which are either Export Controlled or ITAR controlled are underway (or may be underway in the near future) in parts of the XXXX laboratories under the supervision of Professor XXXXX. SAMPLE

JANE DOE shall not access any NASA/MSFC export controlled items. This includes hardware, software and technical data controlled by the International Trafficking in Arms Regulation (ITAR), Export Administration Regulations (EAR), Nuclear Regulatory Commission (NRC), or Drug Enforcement Administration (DEA) regulations. SAMPLE

JANE DOE shall not be exposed to, educated or briefed or access any NASA/MSFC Sensitive but Unclassified, sensitive, proprietary information, data, hardware or software. SAMPLE

3) PHYSICAL SECURITY

JANE DOE will have access to all common areas (e.g. conference rooms etc.) throughout the National Space Science Technology Center (NSSTC)/Cramer Hall. While working at the NSSTC, individuals shall be able to work the times and days of their choice in accordance with NSSTC policies and procedures as approved by their NSSTC supervisor. SAMPLE

ITAR and CUI documents will be stored in hard copy and electronically. Hard copies are to be stored in a locked cabinet and/or security container in a locked office (with limited access). Electronic files are stored on hardware encrypted USB drives which are stored in a locked cabinet and/or security container in a locked office (with limited access). Only project personnel will be allowed access to the ITAR and CUI information. Accessing ITAR and CUI documents will be restricted to isolated computers and servers. SAMPLE

4) INFORMATION SECURITY

The University of Alabama in Huntsville rules requires 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 protection of controlled and sensitive information under this TCP. Controlled data are categorized under the Data Classification Standard as Category I data. All project data and other related digital materials will be strongly

password-protected and encrypted using commercially available encryption technology. The computer(s) on which this data will be stored shall not be connected to any networks. When this computer has reached its usable life, the hard drive will be forensically erased or destroyed using university hard drive destruction services provided by Office of Research Security, Denise K. Spiller, and Security Administrator/Export Control Compliance Officer.

5) PERSONNEL SCREENING

All personnel with access to the controlled technology and their nationality are listed in the TCP Certification Form. Citizenship has been verified through the appropriate channels with Office of Research Security.

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. Additional export control training specific for this project may be conducted by the Office of Research Security (ORS) Export Control Officer. ORS also provides annual training sessions to members of the UAH community. A yearly Export Control Refresher 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 Delores Newton at dn0003@uah.edu (256-824-6048). 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 Controls Officer or the export controls.**

8) ACCESS TERMINATION

Security measures, as deemed appropriate, will remain in effect until the individual no longer requires access or the project has ended, at which time the information will be destroyed or determined to be no longer export-controlled.