Individual Requesting and Responsible for TCP:
Telephone Number: 256-824-
E-mail Address: @uah.edu
Request Date: 2015

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

Project Personnel
List Name(s)  Citizenship  Export Training Date:  Signature:

Is sponsored research involved?

Is a non-disclosure agreements involved? Yes

If yes, identify the parties:

Contact Information:

Attachments:
1. TCP
2. Export Briefing and Certification Form(s) for each person subject to this TCP

Approved By:

______________________________  ________________
Denise K. Spiller                     Date
Security Administrator, Export Controls Officer
TECHNOLOGY CONTROL PLAN (TCP)

1) COMMITMENT
The University of Alabama in Huntsville (UAH) is committed to export controls compliance. The Office of Research Security is responsible for implementation of the Technology Control Plans (TCP) 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 PI Name: xxxxxxx.

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

3) PHYSICAL SECURITY

4) INFORMATION SECURITY
The University of Alabama in Huntsville rules requires all researchers 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 Research Security Administration, 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.

6) TRAINING AND AWARENESS
All personnel with access to controlled information on this project will have completed the online Export Control Certification Web Training and also have completed the Briefing and Certification on the Handling of Export-Controlled Information. Additional export control
training for this project may be conducted by the Office of Research Security (ORS) Export Controls Officer. The ORS also provides annual training sessions to members of the University of Alabama in Huntsville 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 one of the Empowered Official for export controls 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 Empowered Official for export controls.

8) 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 terminated when the information has been destroyed or determined to be no longer export-controlled.