GVSU Technology Control Plan *

In accordance with the export control regulations as specified by the U. S. Department of Commerce Export Administration Regulations (EAR) and the U. S. Department of State International Traffic in Arms Regulations (ITAR), a Technology Control Plan is required in order to prevent unauthorized export of controlled technology deemed to be sensitive to national security or economic interests. This form provides the basic and minimum elements of a Technology Control Plan.

I. General Information

a). Date: _____

b). Principal Investigator: _____

Department/Address: _____

Phone: _____ E-mail: _____

c). Title of Sponsored Project/Activity:

_____

d). Technical description of item/technology/equipment/software to be controlled:

II. Physical Security Plan

Project data and/or materials must be physically shielded from observation by unauthorized individuals operating in secured laboratory spaces, or during secure times blocks when observation by unauthorized persons can be prevented. This would pertain to laboratory management of "work in progress."

a). Location: Describe the physical location of each sensitive technology/item to include building and room numbers A schematic of the immediate location is recommended.

b). 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.)

c). Perimeter Security: Describe perimeter security features of the location of the protected technology/item

III. 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 strictly controlled and managed allowing only authorized persons to access and transmit data over the internet, using only advanced or federally approved encryption technology.

a). Structure of IT Security: Describe the IT setup/system at each technology/item location

* Source: Oklahoma State University, Office of University Research Services, October 2008

III. Information Security Plan, con't.

b). IT Security Plan: Describe in detail the IT security plan, (i.e. passwords, access, firewall protection plans, encryption, etc.

c). Verification of Technology/Item Authorization: Describe how the export controlled technology will be managed and secured in the event of employee terminations, individuals working on new projects, etc.

d). Conversation Security: Describe the plan for protecting information about controlled technology in conversations. Discussion s about the project/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 subcontracts are only to be conducted under signed agreements that fully respect the non-U. S.citizen limitations for such disclosures.

IV. Item Security

Describe the 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.

V. Project Personnel

Identify every person (including their national citizenship) who is determined to have authorized access to the controlled technology/item:

Full Name	**Country of Citizenship**

VI. Personnel Screening Procedures

At a minimum, a review of the entities and denied parties list must be conducted. Controlled technology cannot be shared with any person or entity found on any of these lists. Describe any other screening procedures (i.e. criminal background check, driver's license, etc.). The U. S. Department of Commerce website is: http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm.

VII. Training and Awareness Program

Describe training to be provided to U. S. employees and/or foreign national on the restrictions and measures governing controlled technology

VIII. Self-Evaluation Program

a). Self-Evaluation schedule: describe how often the TCP will be reviewed and evaluated. Plans must be reviewed, at a minimum, on an annual basis.

b). Corrective Action Items: Describe the process to address any findings in the self-evaluation or audits.

ACKNOWLEDGEMENTS

Principal Investigator

Name:

Signature: _____ Date: _____

Department Chair/Unit Head

Name:

Signature: _____ Date: _____

University Authorized Official

Name:

Signature: _____ Date: _____