SDBOR Technology Control Plan (TCP)

Project Title: _____

Principal Investigator: _____ Department: _____

Phone: _____ Email: _____

Description of Controls (EAR/ITAR Category):

Location(s) Covered by TCP:

Is sponsored research involved? Yes ☐ No ☐

If yes, identify sponsor:

Identify Award Number:

Identify any subcontract awards:

Projected end date of project:

I. COMMITMENT AND RESPONSIBILITIES

The South Dakota Board of Regents is committed to export controls compliance. The Empowered Official will assist the Principal Investigator (PI) and researchers with complying with this Technology Control Plan (TCP). The Empowered Official for export controls is Katie Ludvigson, System Export Control Officer, Katie.Ludvigson@sdsmt.edu, 605-394-1687.

II. BACKGROUND AND DESCRIPTION OF THE USE OF CONTROLLED ITEMS

This TCP is required because of one or more of the following conditions exist:

a. Export controlled under an Unclassified project:
   This project may involve access to unclassified export controlled items, materials, equipment, software, data, information or technology.
b. Publication or Foreign National Restrictions:

The project may involve export controlled items, materials, equipment, software, data, information or technology and has publication and/or foreign national restrictions.

III. PERSONNEL ACCESS

Project Personnel- *(Clearly identify every person including their national citizenship, who is determined to have authorized access to the controlled technology. It is the responsibility of the PI to inform the Export Control Officer of any new addition of project personnel. All personnel shall have Export Control training prior to starting work. The TCP will be amended accordingly.)*

Full Name	Country of Citizenship	Job Title/Work Responsibility

a) Are foreign persons authorized to work on this project? (Note: Green Card Holders are considered U.S. Persons for purposes of export laws.) ☐ Yes ☐ No

b) If yes, is an export authorization required? ☐ Yes ☐ No

c) If yes, has one been obtained? ☐ Yes ☐ No ☐ N/A

(NOTE: No foreign persons may begin working on the project until such authorization is obtained and activated.)

a. What is the authorization number? _____
b. What is the expiration date? _____

Personnel Screening Measures- At a minimum, all persons that may have access to export-controlled materials or data must be listed on the TCP and screened against US government restricted persons/entities lists. Screening will be completed by the System Export Control Officer or by the designated campus export control contact.

Custodial Services- Regular custodial services are to ONLY be provided by U.S. Persons in the room and facilities management is made aware of this requirement.

IV. PHYSICAL SECURITY PLAN

Location: (include building and room numbers, lab name, etc.):

Physical Security: If the room has multiple uses, how will the work areas be segregated to ensure there are no inadvertent transfers of project information or details? (provide a description of your physical security plan designed to protect the item/technology from unauthorized access, (e.g. secure doors, limited access, security badges, locked desks or cabinets, secure computers, access to keys etc.):

Individuals with keys or key cards are expressly prohibited from permitting others to use their keys or key cards for access to the research site. Doors to secured areas may not be propped or left open.

Item Storage: How will the project equipment be stored? (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):

Destruction or Return of Materials: Describe how the export controlled materials will be handled at the end of the project or when they are not needed anymore (shredding, file wipes, destroy hard drive, return to sponsor, etc.).

Marking Documents and Hardware- How will controlled equipment be tagged or identified? All [ITAR or EAR] restricted documents and hardware (when possible) are to be clearly marked with "This document/hardware/software is Export controlled. Violation of export laws are subject to severe criminal penalties."

Visitors and Guest Access- The researchers and staff who are authorized to enter the room when export controlled material is present will escort all visitors and keep visitor logs during the time export controlled material is in use. The campus export control contact must be contacted in advance of the visit to approve all visitors prior to granting access to the room and will document citizenship of all visitors when making access determinations.

Procurement- Procurement of parts, tooling and equipment specifically designed, developed, configured, adapted, or modified for use with an ITAR-controlled item must be purchased by suppliers and vendor who can certify they are ITAR-compliant.

Photography- Non-work-related photographs of export-controlled items are strictly prohibited. Photos are to be stored in secure locations.

V. COMPUTING AND INFORMATION SECURITY

1. How will project-related laboratory notebooks and any other hard copy materials be stored?

2. Where will electronic data be stored and who will have access to the data?

3. How will access to electronic data be restricted to only those individuals authorized to access the data?

4. How will the information/deliverable be transmitted to the sponsor?

5. Who is the assigned IT person? [Must be a U.S. Person]

Note: Password protected files not stored on a network do not have to be encrypted. Any files removed from this system by any media will be encrypted. Virus protection software must be provided for these computers. If isolation is not possible, 128-bit or better encryption will be utilized to protect information.

Removable hard drives may be used for data back-up. When not in use, the back-up removable drives must be securely locked away. Only person(s) with key access:

Note: Any computer hard drives containing sensitive information will be formatted at the end of the contract plus overwritten three times with a DOD disk-wipe program.

SPECIAL NOTE REGARDING EMAIL - Export-controlled information/deliverables should not be distributed or received utilizing email without encryption under any circumstances. Gmail accounts are not secure and should never be used as a form of communication for export-controlled projects.

6. Technical Data Marking - Documents containing export-controlled technical data must be marked with one of the following legends:
   a) "This information is subject to the controls of [pick one: the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR)] and should not be distributed to non-U.S. persons or outside of the U.S. without prior permission of the U.S. State dept."
   b) "ITAR- [or EAR-]controlled – do not distribute to non-U.S. Persons."

7. Clean Desk Policy - A clean-desk policy is in effect. Hard copies of project-related information should be locked in a secured/locked location (secured drawer or cabinet) when not in use and at the end of every day.

8. Controlled Information Security - Export controlled information may not be posted on networks with uncontrolled shared access. A secure ITAR designated system is used as the primary storage for all ITAR materials. The IT Security Office is responsible for ensuring that the system is secure. Storage and backup of the ITAR data is stored on an encrypted device. No open remote storage of such documents is permitted (i.e. Dropbox or Google drive). The device is secured in a locked cabinet when not in use. All ITAR data and documents must be password protected and encrypted. Access to computers used for projects with ITAR material is controlled, and ONLY approved project personnel may be granted access. Information security shall be in compliance with NIST 800-171 requirements by December 31, 2017.

   a) Remotely working on ITAR restricted materials in public locations (eg. coffee shops, airports, computer labs, etc.) is prohibited because the citizenship of onlookers cannot be verified.
   b) Transfer of ITAR restricted materials to remote storage like Dropbox or Google Drive is prohibited.
   c) Transfer of ITAR controlled materials to a laptop, personal computer, or portable drive (USB drive) is prohibited.

VI. INTERNATIONAL TRAVEL

Will there be any international travel associated with this project? ☐ Yes ☐ No

If so, when and where, if known:

Contact the Empowered Official as far in advance of the trip as possible.

Computers or other electronic storage devices containing restricted information should not normally be used for travel. If a computer is necessary for international travel, all unnecessary technical information not required for the trip should be removed and any information which is required must be authorized for the destination and end use.

For meetings, foreign travel, emails, symposiums, etc., where unlicensed controlled technology is potentially discussed, prior approval will be sought from (sponsor) and the (government agency) and licenses obtained if necessary.

VII. TRAINING AND AWARENESS

Export control training should be done periodically. The Principal Investigator should complete export control training and all project personnel shall be briefed on export controls. Please indicate any and all export control training you have received and the date(s):

VIII. CONVERSATIONS, DISCUSSIONS AND PRESENTATIONS

Conversations and discussions about the project or work products are limited to the project team. Conversations and discussions should be held only in areas where unauthorized personnel are not present. Conversations and discussions may not take place in public locations where non-US person may be present.

Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations without prior approval of the Directorate of Defense Trade Controls (DDTC) or the U.S. Department of Commerce, Bureau of Industry and Security (BIS). Note- If a license is required the process may take three to six months or longer. Public release of information shall not occur until any required permission or government approval is received by the DDTC or the BIS.

IX. PUBLICATION

In most cases, restricted research will contractually require that project personnel shall not release or disseminate any information pertaining to the project without the prior written approval of the sponsor, excluding information already in the public domain. In the rare case that there is not a contractual publication restriction and the project involves controlled items, research results and publications generated from the controlled items are still subject to the approval of the sponsor. Therefore, when publications of projects that involve controlled items are subject to the approval of the sponsor, the impact of such restrictions should be considered prior to employing graduate students and tenure track faculty. Publications (including but not limited to theses, dissertations or journal publications) may be delayed or denied based on the approval of the sponsor or US government.

X. COMPLIANCE ASSESSMENT

As a critical component to ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the System Export Control Officer, Katie Ludvigson, 605-394-1687 or katie.ludvigson@sdsmt.edu. Any changes to the approved procedures, project personnel having access to controlled information covered under this TCP will be cleared in

advance by the System Export Control Officer.

XI. REPORTING AND RESPONSIBILITIES

Any person having knowledge of a potential violation or noncompliance with the provisions of this plan or any applicable export control obligation must immediately report the circumstances surrounding the activity to the System Export Control Officer at 605-394-1687 or katie.ludvigson@sdsmt.edu.

Certification: I hereby certify that I have read and understand this Technology Control Pan and my obligations under federal law and SDBOR policies regarding the item, technology, or technical data identified in this TCP. I agree to take the actions set forth in this TCP and, if applicable, to comply with the terms of any license governing the item, technology or technical data and the terms in any contract regarding such item, technology or technical data.

Principal Investigator Date

Department Chair Date

Empowered Official Date