FOREIGN NATIONAL TECHNOLOGY CONTROL PLAN
PROJECT: [Insert Title]
USCERA PROPOSAL NUMBER: [Insert Proposal Number]

Per the Project solicitation, the agreement and/or the Sponsor this Project has been determined to be export controlled and subject to the [Insert subject regulations (ITAR, EAR, 10 CFR Part 810, etc.)]. In order to comply with the [Insert EC regulation] the following will be addressed:

Accessibility of information

Only those on the Project will have access to the items, information and/or software either provided by the Sponsor or developed/generated under the Project.

No non-US persons will be/have:

a. Allowed on Project;
b. Involved in meetings concerning Project;
c. Access to items, information or software provided by the Sponsor or developed/generated under the Project in any form or format;

Those authorized to be on the Project will be instructed not to share or release information pertaining to the Project in any form or format (written, verbal or otherwise) to those not authorized on the Project.

Location of Work

Research will be conducted in [Insert building/buildings and room number/s]. The system containing the export-controlled information will be a Virtual Desktop within the Carolina Enclave for Secure Research (CESR), a NIST 800-171 Rev 1 compliant research environment, while the TCP is in force. CESR Client Access machines will be located in Insert building/buildings and room number/s]. [Identify any information, materials, equipment etc. that is controlled and describe where it will be maintained.] This/These area[s] will be off-limits to non-US persons while the TCP is in force.

Physical Security

Protected data will be stored within the Carolina Enclave for Secure Research, either in the USC DoIT Data Center or area data centers listed above, or in approved local Secure Research Labs or offices that comply with CESR standards. Outside of active working periods, [list all controlled items, materials, equipment, data, software to be used or developed on the project] as well as any portable media containing export-controlled information or software will be locked in a file cabinet fitted with a locking bar and located in [Insert building and room number]. The door lock will be changed to a separate key, and copies of this room key, as well as the file cabinet keys, will be issued only to the following personnel:

- [Insert PI Name] (PI)
- [List other persons with access as well as their title]
- [Insert Department IT] (IT)

A warning notification will be displayed in the hallway outside [Insert building and room number] indicating that it is a limited access area and only authorized personnel may enter the area while this room is in use for this project. Unauthorized individuals will be reported to the PI and their presence will be reported to the Sponsored Awards Management Office (Brandi Boniface 803 777-8749) as a potential violation. Sponsored Awards Management will conduct an internal review to determine if a violation occurred. Based upon the information identified in the internal review Sponsored Awards Management will notify law enforcement and the appropriate US Government agencies, as necessary.

All hardcopy information or data provided by the Sponsor will be stored in a locked file cabinet or drawer when not in use. A log sheet will be used to record each instance of the system being removed from the locked cabinet for use.

Computer System

The Department IT person [Insert Department IT Name] will set up a CESR Client Access computer system which meets the CESR standards. This system will be used to access the assigned CESR Virtual Desktop systems used to process, manipulate, analyze, or store the protected data within the CESR (Carolina Enclave for Secure Research) environment.

[this section is to be completed by the Department IT in collaboration with the PI and in accordance with NIST SP 800-171 Rev 1 **for other systems housing protected data outside of the CESR Virtual Environment]**

Login access to the will be limited to the following personnel:

- Insert PI Name] (PI)
- [List other persons with access as well as their title]
- [Insert Department IT] (IT)

Administrative access to the CESR environment is limited to the following personnel and groups:

- [Department IT Name]
- The DoIT Research Computing Group
- The DoIT Networking Infrastructure Group
- The DoIT Datacenter Operations Group
- The University Information Security Office

If export-controlled information is to be made available outside of the system, such as for delivery to the project sponsor, the Secure File Transfer Server in the CESR will be used. Other project deliverables will be sent to the project sponsor via [list delivery methods] as specified.

A schedule will be established to ensure regular preventative maintenance and data backups on systems as required by the CESR standards.

Shared Resources

Shared resources such as scientific equipment or instruments will be off-limits to non-US persons while in use for this project. A warning notification will be displayed on the door of [Insert building and room number] indicating that it is a limited access area and only authorized personnel may enter the area while this room is in use for this project. Where practical, door locks or door card access restrictions will be adjusted to limit entrance to the room to project personnel only. Unauthorized individuals will be reported to the PI and their presence will be reported to the Sponsored Awards Management Office (Brandi Boniface 803 777-8749) as a potential violation. Sponsored Awards Management will conduct an internal review to determine if a violation occurred. Based upon the information identified in the internal review Sponsored Awards Management will notify law enforcement and the appropriate US Government agencies, as necessary.

Once finished, all protected data will be securely wiped from any controlling computers or machines before returning the shared resource to general use.

Portable Storage **[this section is to be completed by the Department IT in collaboration with the PI]**

It is not recommended that removable hard drives, jump drives or other mobile media be used to store export-controlled data. However, if it is used, such devices must be encrypted using FIPS-compliant BitLocker encryption. If data is to be made available outside of the system, such as for delivery to the sponsor, it will be encrypted using FIPS-compliant software, such as Bitlocker with FIPS-compliance enabled.

Any decryption passwords should be shared separately via a secure medium, such as encrypted email or direct telephone communication.

All hardcopy information or data on removable media provided by the Sponsor or containing protected data will be stored in a locked file cabinet or drawer when not in use. A log sheet will be used to record each instance of removable media being removed from and returned to the locked cabinet or lockbox for use.

Conversation Security

Projects conducted in facilities shared with other projects and personnel must also consider reasonable plans or procedures to prevent unintended or unauthorized transfer of export-controlled information via conversations. [Describe either why restrictions on conversation are not applicable or the procedures for restrictions on conversation to be used. Example: Project personnel will be instructed to hold conversations pertaining to the project in dedicated office spaces or conference rooms, behind closed doors. Conversations pertaining to protected information will not be held in the presence of personnel not assigned to the project.]

Decommissioning

Upon termination of the research, any media used to store export-controlled data will be kept in a secure cabinet for safekeeping until no longer needed. It will then be destroyed in such a manner as to ensure that recovery of export-controlled data is not possible. Documentation recording the proper destruction of materials will meet CESR standards.

Project-specific decommissioning requirements or archival or retention of protected data will follow the project's data management plan or instructions in the project contract. Protected data must still be protected upon project completion, unless otherwise specified by the project sponsor.

Updates and Changes to Personnel

PI will notify Sponsored Awards Management (SAM) of any expected changes in personnel at least 15 days prior to the change.

PI will obtain SAM approval prior to adding any non-US Persons to the effort. SAM will obtain US Government export control licenses or other authorizations as appropriate.

PI will notify SAM of any changes to the scope at minimum 15 days before the new scope is implemented. PI will not allow non-US persons to work on or have access to the new portion of the effort pending review of revised scope and receipt of US Government export control licenses or other authorizations addressing the revised scope as appropriate.

PI will ensure that any new persons added to the project have attended an export control training session and all persons on the project attend and refresher training once every 12 months.

PI will ensure that any new persons added to the project have reviewed this Technology Control Plan and have signed attachment A indicating they have read and understood its and obligations.

Special Items

The efforts under this TCP are subject to the DFARS 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019) clause. The PI in collaboration with the Department IT and SAM will ensure that the effort complies with the DFARS 252.204-7012 requirements.

[The Remainder of this Page has been Intentionally Left Blank.]

FOREIGN NATIONAL TECHNOLOGY CONTROL PLAN
PROJECT: [Insert Title]
USCERA PROPOSAL NUMBER: [Insert Proposal Number]

Principal Investigator

By: _____

Name:

Title: *Principal Investigator*

Date: _____

Department

By: _____

Name:

Title: *Chair,*

Date: _____

College

By: _____

Name: Michael Matthews

Title: *Vice-Dean, CEC*

Date: _____

Department IT

By: _____

Name:

Title: *System Administrator,*

Date: _____

FOREIGN NATIONAL TECHNOLOGY CONTROL PLAN
PROJECT: [Insert Title]
USCERA PROPOSAL NUMBER: [Insert Proposal Number]

Attachment A:

I hereby certify that I have read and understand the provisions of the above Foreign National Technology Control Plan, as well as understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, information, software or items either provided by the Sponsor or generated under this Project to unauthorized persons.

Print name:_____School/Dept_____

US Citizen___ Green Card___ Foreign National/ Country of Origin_____

Signature: _____

Print name:_____School/Dept_____

US Citizen___ Green Card___ Foreign National/ Country of Origin_____

Signature: _____

Print name:_____School/Dept_____

US Citizen___ Green Card___ Foreign National/ Country of Origin_____

Signature: _____

Print name:_____School/Dept_____

US Citizen___ Green Card___ Foreign National/ Country of Origin_____

Signature: _____

Print name:_____School/Dept_____

US Citizen___ Green Card___ Foreign National/ Country of Origin_____

Signature: _____