Federal Regulations

Projects/activities involving the use of Export-Controlled Information (ECI) come under the purview of either the State Department’s International Traffic in Arms Regulations (ITAR)\(^1\), or the Department of Commerce’s Export Administration Regulations (EAR)\(^2\).

It is unlawful under the EAR or ITAR to send or take Export-Controlled items or information out of the U.S. This includes disclosing information orally or visually, or transferring export-controlled items or information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, an export license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

University Policy

In addition to Federal Regulations, the University of North Carolina at Charlotte (UNC Charlotte)'s own Policy #316 “Export Control”\(^3\), reiterates the University’s commitment to comply with all United States export control laws and regulations. Links to additional information about EAR and ITAR regulations can be found on UNC Charlotte’s Office of Research Compliance & Ethics website.\(^4\)

Per University Policy #316, the Vice Chancellor for Research and Economic Development serves as the Empowered Official for export control matters and has final approval authority for Technology Control Plans (TCPs). The Export Controls Officer in the Office of Research Compliance provides services/advice as needed on export control issues and Technology Control Plans.

Technology Control Plans

A TCP provides guidelines to ensure that the information is not transferred to a foreign person or persons unless approved by license with the Department of State, Office of Defense Controls (ODTC) or Department of Commerce as applicable.

Pertinent technical information, data, materials, software, or hardware, i.e.; technology generated from projects involving the use of Export-Controlled Information must be secured from use and/or observation by unlicensed non-U.S. citizens. Security measures must be appropriate to the classification involved.

In order to prevent unauthorized exportation of protected items/products, information, or technology deemed to be sensitive to national security or economic interests, a Technology Control Plan (TCP) may be required. The following pages provide the basic template for a TCP. The TCP shall include a physical and information security plan, personnel screening procedures and a process for carrying out the research in a controlled environment.

UNC Charlotte requires all researchers to ensure that sensitive digital research data is appropriately protected. Any requirements explicitly outlined in the contract or NDA, such as technology controls, data classification, encryption, network access (or lack thereof), non-disclosure, secure destruction, etc., must be adhered to at all times. For more complete information and assistance in setting up the Technology Control Plan for your project, contact tcp@uncc.edu.

---

\(^1\) See ITAR regulations at [pmddtc.state.gov/regulations_laws/itar_official.html](http://pmddtc.state.gov/regulations_laws/itar_official.html)
\(^2\) See EAR regulations at: [http://www.access.gpo.gov/bis/ear/ear_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html)
\(^3\) See UNC Charlotte’s University Policy #316 at: [http://legal.uncc.edu/policies/up-316](http://legal.uncc.edu/policies/up-316)
\(^4\) See Office of Research Compliance & Ethics at: [http://research.uncc.edu](http://research.uncc.edu)
Process for Implementation of the UNC Charlotte Technology Control Plan (TCP)

Technology Control Plans (TCP) may be implemented if there is a Non-Disclosure Agreement (NDA), or a Data Security Plan requested for the research. In some instances, a TCP may be used to satisfy security requirements of Third Party Proprietary Information, or if there are Publication Restrictions, a “request to review before release” clause, a “No Foreign National Restriction” and if any of the technology/equipment/information is controlled by the Commerce Control List (CCL), covered in International Traffic in Arms Regulation (ITAR) or if classified information involved.

EXPORT CONTROLS TRAINING must be completed by every individual on a project with a TCP — including PI & students — before working on the project or being charged to the project. Go to: http://www.citiprogram.org to establish an account. Select the “CITI Export Controls Course”. You must affiliate with UNC Charlotte in order for the Export Controls office to track your training completion.

ALL MEMBERS OF THE RESEARCH TEAM will be required to read, understand, and sign the TCP before funds will be released and before anyone can work on, or be paid on, the project.

NOTE: Foreign Nationals may not work on projects ineligible for FRE without an export license. Additionally, students (including US citizens) may not work on any project ineligible for the Fundamental Research Exclusion for their thesis or dissertations.

INSTRUCTIONS

1. **Part I**: Provide contact information for the person requesting and responsible for the TCP as well as for each person who will have access to export controlled subject matter. Indicate the start/end dates for the project.

2. **Part II**: Provide a description of the technology/technical data to be secured and the measures being used to secure it.

3. **Part III**: Prepare a separate Certification for each person listed in Part I who will have access to Export Controlled subject matter.
   a. Discuss the following with all personnel listed in Part I:
      i. The Technology Control Plan (as detailed in Part II).
      ii. Each section of Part III.
   b. Ask each person to:
      i. Initial each section.
      ii. Sign the Certification at the end of the document.

4. **Submit Parts I, II and Part III to the Export Controls Officer in the Office of Research Compliance.** If you have any questions or concerns about your Technology Control Plan contact the Export Control Officer at tcp@uncc.edu or 704-687-1877.
# Technology Control Plan (TCP) Certification

## Part I: Project Information

1. **Individual Requesting and Responsible for TCP:**
   - Telephone Number:
   - E-mail Address:
   - Request Date:

2. **Project Title:**
   - NORM Proposal Number:

### Description of Controls:

*(Specify EAR/ITAR Category)*

### Location(s) covered by TCP

*(Add rows if needed)*

   - Building:
   - Room #:

### Project Personnel

List all personnel who will have access to export controlled subject matter (add additional row(s) if needed)

<table>
<thead>
<tr>
<th>List Name(s) Below <em>(Last Name, First Name, MI):</em></th>
<th>List citizenship(s)</th>
<th>Permanent Resident Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Is sponsored research involved?**

- [ ] YES
- [ ] NO

*If YES, identify sponsor:*

**Projected START and END dates:**

- **Start Date:**
- **End Date:**

**Is a non-disclosure agreement involved?**

- [ ] YES
- [ ] NO

*If YES, identify the parties:*

**Contact Information:**

**Attachments Submitted**

- [ ] TCP
- [ ] Export Briefing and Certification Form(s) for each person subject to this TCP

**APPROVED BY:**

______________________________  Date: ___________________

Robert G. Wilhelm, Ph.D.  Vice Chancellor for Research and Economic Development
Part II: Technology Control Plan (TCP)

1  Principal Investigator • Project Title • Proposal Number

The Principal Investigator responsible for and committed to ensuring compliance with this TCP is:

<table>
<thead>
<tr>
<th>LAST NAME:</th>
<th>FIRST NAME:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPT:</td>
<td>BLDG/ROOM #:</td>
</tr>
<tr>
<td>EMAIL:</td>
<td>PHONE:</td>
</tr>
<tr>
<td>PROJECT TITLE:</td>
<td>NORM PROPOSAL #:</td>
</tr>
</tbody>
</table>

NOTE: UNC CHARLOTTE REQUIRES all researchers to ensure that sensitive digital research data is appropriately protected. Any requirements explicitly outlined in the contract or NDA, such as technology controls, data classification, encryption, network access (or lack thereof), non-disclosure, secure destruction, etc., must be adhered to at all times.

2  Description of the Use of Controlled Items and Information

In the text boxes provided below, please provide description of the project, any third party technology to be provided for the research and how ‘third party’ deliverables will be delivered to UNC Charlotte:

A. Provide a brief description/overview of the project.

B. Describe any “third party” technology, sensitive data, equipment and materials which will be provided for your research.

C. Describe how the “third party” deliverables will be delivered to UNC Charlotte.

3  Physical Security

Describe the physical security controls that will be used to prevent unauthorized access to secured areas and to protect project materials and computers. At a minimum, these controls should address how you plan to do the following:

- Ensure that project materials (physical or digital) do not leave the secured areas (including via the network).
- Ensure that work for this project is done within secured areas.
• Mark all physical materials (e.g. hardcopy, removable media, etc.) as “Export Controlled”, “Proprietary”, and/or “Subject to a Non-Disclosure Agreement (NDA)” as appropriate. The plan should provide that materials be physically secured from access to unauthorized personnel when not in use.

• Prevent non-U.S. persons (i.e., Foreign Persons) from viewing or having access to any project data (physical or digital) or secured area(s) (including maintenance, cleaning, and others).

• Ensure that only project members are present in the secured areas when work on this project is being performed.

In the text box provided below, please describe the physical security controls to be implemented:

Physical Security Controls for this project include:

4 Information Security

Describe the information security controls that will be used to protect sensitive project data. Based on the requirements outlined in the contract, subcontract or NDA, such as technology controls, data classification, encryption, network access (or lack thereof), non-disclosure, secure destruction, etc., controls may include some or all of the following:

a) Encryption of Project Data: Data related to this project must not be sent unencrypted over any networks. All data stored on computers and removable media must at least be encrypted, utilizing a whole disk encryption product wherever feasible.

b) Dedicated Project Computers: Project computers must be dedicated exclusively for work that is covered by this Technology Control Plan and not be general-purpose machines.

c) Non-Networked Computers: Project computers should be non-networked unless network connectivity is required for project work. If network connectivity is required, project computers should be configured to deny all non-essential inbound and outbound traffic. Network connectivity must be restricted to the maximum extent feasible. Apple/MAC addresses for all Ethernet and wireless interfaces must be provided to ITS.

d) No Internet Access for Project Computers: Project computers should not be Internet accessible unless explicitly allowed by the data owner. If project computers are to be Internet accessible, operating system and application patches must be applied in a timely manner. If applications provide an automatic update feature, it should be utilized.

e) End-of-Project Procedures: At the end of the project and/or when project computers reach their usable life, physical media (e.g. hard drives, USB drives, etc.) must be forensically erased or destroyed using university hard drive destruction services.

All project computers must have adequate security controls in place. If you have questions or are not sure about the type/level of security controls needed, contact the Export Control Officer at tcp@uncc.edu who will assist and be your liaison with the ITS Security Office in this process. Any exceptions to the TCP must be documented in writing and approved by the Export Controls Officer.

In the text box provided below, please explain, in detail, what information security controls will be used to protect sensitive project data.

Describe information security controls to be used to protect sensitive project data:

5 Personnel Screening, Training and Awareness

All personnel listed in Part I of this TCP and with access to export controlled information, technology, software, or items on this project must:

• Read Part II “Technology Control Plan”;
• Provide their signatures in Part III, “Briefing and Certification on the Handling of Export Controlled Information” indicating that they have read and understand the information in Part II detailing the technology control plan to be implemented.

Additionally, all personnel with access to digital data/information stored on their university computer must read and agree to follow the UNC Charlotte Policy Statements for Protecting Sensitive Digital Research Data listed below:

1. Data and Information Access and Security (Policy #311) and applicable sub policies 311.3, 311.4, 311.7, 311.9
2. Electronic Communication Systems (Policy #304)
3. Network Security (Policy #303)
4. Proprietary Software (Policy #601.14)
5. Responsible Use of University Computing and Electronic Communication Resources (Policy #307)
6. Web Communications (Policy #302)

6 Compliance Assessment
As a critical component to the University’s ongoing compliance monitoring efforts, self-evaluation is an internal assessment process whereby procedures are reviewed by the researcher and any findings reported to the Export Controls Officer at tcp@uncc.edu (704.687.1877).

These internal assessments should be done by the research on a quarterly basis for the duration of the research project. The Export Controls Officer may also conduct more frequent evaluations and/or training to monitor compliance of the TCP procedures.

Any changes to the approved procedures or changes in personnel having access to controlled information covered under this TCP must be cleared in advance by the Export Controls Officer.

Upon review of this Technology Control Plan by Export Control Officer, this TCP will be submitted to the Empowered Official for Export Controls for review and signature prior to implementation.

7 Project Termination
Security measures will be required for export controlled information and items after the project termination. NOTE: These are project-specific and are dictated by the awarding agency and are typically specified in the contract/award.

Describe the security measures to remain in effect for Export Controlled information and items following termination of the project.

Technology Control Plan reviewed by the Export Control Officer only after Parts II &III are completed.

REVIEWED BY: ____________________________________________________ Date_____________________

John Jacobs, Export Controls Officer
Part III: Project Personnel: Briefing and Certification

on the Handling of Export Controlled Information

(Complete and submit a separate Certification for each person listed in Part I of this document.)

<table>
<thead>
<tr>
<th>Research Project Title:</th>
<th>NORM Proposal #:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Name:                   | N:                |
| (Last Name, First Name, MI): |                  |
| List citizenship        | PH:               |
| Permanent Resident Status | Email:           |
| Department:             |                  |

NOTE: For the purposes of this certification, a Foreign Person is a person who is not a U.S. citizen or lawful permanent resident alien (Green Card Holder) as defined by U.S 8 U.S.C. 1101(a) (20)., or who is not protected individual as defined by U.S 8 U.S.C. 1324b(a) (3).

Please initial each section:

I. I understand the following:
   - Export Control Regulations are United States laws that regulate and restrict the release of critical technologies, technical data, software code, equipment, chemical and biological materials, and other materials information and services to Foreign Persons and foreign countries for reasons of foreign policy and national security.
   - An export can be any of the following:
     - Shipment of a controlled commodity, equipment, material, or software outside of the U.S.
     - Discussion or disclosure of controlled technology or technical data to a Foreign Person, whether in the U.S. or abroad.
     - Performing technical assistance or defense services for or on behalf of a Foreign Person, whether in the U.S. or abroad.
   - Exports within the U.S. are considered to be a "deemed export" to the foreign person’s home country.
   - A Foreign Person is a person who is not a U.S. citizen or lawful permanent U.S. resident.
   - The ultimate end-use or end-user of the information, software, or item is not determinative of whether it is Export Controlled.

II. I understand that the following are not “export controlled”:
   - Basic marketing information on function or purpose; general system descriptions; information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities; published information in the public domain; and published patent information.
   - Information developed as a result of fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published, without any publication restriction or pre-publication review requirement.

III. I understand that it is unlawful to do any of the following:
   - Send or take export controlled information, technology, software, or items out of the U.S.;
   - Disclose, orally or visually (including by email, fax, phone, etc.), or
   - Transfer to a foreign person inside or outside the U.S. without prior authorization from the cognizant U.S. government agency.
I certify that I understand and agree to follow:

- The security measures designed and outlined in Part II of this TCP:
- The following UNC Charlotte Policies:

  7. Data and Information Access and Security (Policy #311) and applicable sub policies 311.3, 311.4, 311.7, 311.9
  - Electronic Communication Systems (Policy #304)
  - Network Security (Policy #303)
  - Proprietary Software (Policy #601.14)
  - Responsible Use of University Computing and Electronic Communication Resources (Policy #307)
  - Web Communications (Policy #302)

**INDIVIDUAL CERTIFICATION:**

By my signature below, I certify that

- I am aware that this project involves the use of U.S. Export Controlled information, equipment, or software and
- I am aware that the International Traffic in Arms Regulations (ITAR) 22 CFR 120-130, the Export Administration Regulations (EAR), or other U.S. Export Control regulations apply to the project listed above.
- I have read, understand and agree to follow the Technology Control Plan as described in Part II of this document and the UNC Charlotte Policies listed above.
- I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export Controlled information, technology, software, or items to unauthorized persons.

Individual’s Signature  ___________________________________________  Date: ________________

Printed Name:  _____________________________________________________________

**PRINCIPAL INVESTIGATOR ACKNOWLEDGMENT:**

Please initial each section:

I. I understand that the law makes no exceptions for foreign graduate students or visiting scientists.  

II. As the Principal Researcher on this project, I understand:

- I may be held personally liable for civil or criminal violations of the U.S. Export Control Regulations;
- I must be clear on the requirements and exercise reasonable care in using and sharing Export Controlled information, technology, software, or items with others.
- Any changes to the approved procedures or changes in personnel having access to controlled information covered under this TCP must be cleared in advance by the Export Controls Officer.

I certify that:

I have met with the above individual and through our discussion, they have demonstrated to me their understanding of the scope of this Technology Control Plan (TCP) and have agreed to comply with the entire requirements set forth in this TCP.

Principal Investigator’s Signature  ___________________________________________  Date: ________________

Printed Name:  _____________________________________________________________