**TECHNOLOGY CONTROL PLAN**

**Template**

1. **Statement of Institutional Commitment**

Rowan University(RU) is fully committed to complying with applicable export control laws. To ensure compliance with these laws, Rowan University’s projects and programs will be managed in accordance with applicable Federal laws, rules and regulations as well as “Institution’s Export Control Policies and Program” in compliance with U.S. Export Controls: Responsibilities of Faculty, Staff and Students’ dated July 11, 2014. These govern to the extent of any inconsistencies with the Institution’s Information and Guidelines on United States Export Control Laws dated 6/10/2004.

This Technology Control Plan (TCP) identifies the specific measures that will be taken by the responsible parties at the <Enter name of department/center/office and building name and laboratory location(s) Here>. The responsible parties are empowered to ensure compliance and security with the requirements described in this TCP.

This project is conducted under the provision of Fundamental Research Exclusion. There is no actual export of items to foreign person or foreign countries.

1. **Responsible Parties**

**Empowered Official:** Vice President Research

**Faculty or Staff:**

**Division of University Research:** Director of Research Compliance

1. **Scope**

Investigate various applications of <Include description here>. How the technology can be customized to support <Include description here> activities and to define specific technology to be used to determine <Include description here>.

1. **Project Description**
2. **Deliverables**
3. **Covered Items and Information**

The following items or information have been determined to be subject to export control requirements which require that the University place limitations on who may have access to or use the items or information, hereinafter called *Covered Items and Information*. A variety of factors must be taken into account to determine who may have access to *Covered Items and Information*; for this reason, only individuals who are identified in Appendix 1 embedded in this TCP and have been approved by the Empowered Official may have access. A list of the *Covered Items and Information* that will be protected under this TCP is provided in the exemplified table below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name or Description** | **Type**  | **Jurisdiction** | **Classification**  |
| Need to know what equipment, software, computers, etc.  | Microsoft Windows XP, Windows 7, Vista, Mac OS X, or Linux with the latest security service pack and patches; similar requirements apply to servers and other devices. | EAR | Unclassified |

As a result of this determination, the Responsible Parties, identified above, developed this TCP to ensure that *Covered Items and Information* are adequately protected from disclosure to foreign persons without an approved license, valid license exception, or other written government approval.

1. **Security Overview**

The Information Security Office (ISO) is responsible for the governance and oversight of information security as it pertains to this TCP. This includes both the physical and logical security of *Covered items and information*.

“One Lock” is the principal of securing items and information by using at least one mechanism to prevent access by unauthorized persons. This is the requirement for safeguarding the *Covered Items and Information*, listed above. Methods for obtaining at least “one lock” are described in the physical and information security sections below. Engineering Clinic students and faculty are responsible for safeguarding *Covered Items and Information* at all times by having “one lock”; this includes preventing visual access if such access could provide technical information about an item.

1. **Physical Security**
2. *Work Area.* <Insert name of building here> laboratory where the work is to be performed with *Covered Items and Information* shall have restricted access. Restricted access is defined as having a clearly defined perimeter, which is adequate to protect against oral, in the case of discussions involving *Covered Information*, and visual disclosure of the *Covered Items or Information*. Physical barriers are strongly recommended but are not required as long as oral and visual disclosure can be prevented. Faculty, staff and students in the <Include name of laboratory here> laboratory shall be responsible for challenging all persons who may lack appropriate access authority.

Specific Location where work will be performed with the covered items and information is:

 Example:

South Jersey Technology Park at Rowan University

107 Gilberth Parkway

Mullica Hill, NJ 08062

Room # ………….

1. *Storage.* All export *Covered Items and Information* (hard copies) will be secured in a locked room, storage device or container when not in the personal possession of approved project personnel. Keys or combinations to storage containers used to secure *Covered Items and Information* will only be issued to the approved project personnel authorized on this TCP. Electronic devices containing *Covered Items and Information* will be physically secured or in the possession of an approved user at all times. *Note: Security of electronic files is addressed in the Information Security section, below, rather than here.*
2. *Marking.* Whenever possible *Covered Items and Information* should be clearly marked with an appropriate warning, for example: *WARNING - This contains EAR-controlled technical data. Access or dissemination in violation of the EAR may result in severe administrative (institutional) and criminal (individual) penalties. Contact the Division of University Research, Office of Research Compliance, if you find this item/document unsecured.* When physical space is limited, an abbreviated warning may be used, for example: *Export Controlled - EAR*. Watermarks, headers or footers may be used to mark electronic documents. Compact Discs and other electronic devices such as USB flash drives should marked as described in this paragraph.
3. Description of the markings or warnings that will be placed on covered items:

*WARNING - This contains EAR-controlled technical data. Access or dissemination in violation of the EAR may result in severe administrative (institutional) and criminal (individual) penalties. Contact the Division of University Research, Office of Research Compliance, if you find this item/document unsecured.*

1. **Logical Security**
2. *Computers****.*** All computers used to access or store *Covered Items and Information* must run as exemplified here: Microsoft Windows XP, Windows 7, Vista, Mac OS X, or Linux with the latest security service pack and patches; similar requirements apply to servers and other devices. Generally speaking only approved project personnel should be designated users of computers and servers used to access or store *Covered Items and Information* and a valid account and password must be provided to gain access. Only approved project personnel retain this login information and no other login accounts are created. Both failed and successful logins are logged internally. Firewalls are installed on all computers to secure and monitor network access to/from the computer. If the firewall must be disabled to allow proper data collection, wired and wireless internet connections must be disabled. *Note: Administrative access by central, school or departmental IT personnel are limited to US Citizens.*

List of IT resources (computers, servers, systems, etc) that will be used to store or process Covered Items and Information.

* <Identify IT resources here>

List of individuals such as custodians and maintenance personnel, administrative personnel and IT personnel who are not Project Personnel.

* <List non-Project Personnel here>

Description of project specific security methods, devices or procedures that will be employed to assure computer security.

* <Identify project specific security methods, devices or procedures here>
* The South Jersey Technology Park at Rowan University is subject to all Rowan University Information Security Policies and governed by the Rowan’s Information Security Office.
1. *Data Storage and Transmission.* Example: The ORTS Desktops will be stand-alone computers without connectivity to the internet, local network, or printers. External portable hard drives or flash drives are NOT recommended for data storage unless when physical storage is employed when they are not in use. Drives and devices used to store *Covered Items and Information* are password protected or encrypted. For data storage on drives with network access or backup servers, the *Covered Items and Information* are secured by encryption and password protection. Email will not be used for the transfer of *Covered Items or Information* subject to the EAR. A secure file transfer method (SSH/SCP/SFTP/SSL) or mailing a disk or flash drive is NOT preferred methods to transfer *Covered Items and Information* in electronic format. *Note: Emailing Covered Items or Information subject to control regimes other than the EAR will be considered on a case-by-case basis, but is not authorized unless specified below; when authorized to use email, the sender's is responsible for ensuring that the recipient is physically present in the US at the time of transfer.*
2. *Supercomputing and Cloud Computing.* Unless specified below no supercomputing or cloud computing facilities or services will be used to store, process or transfer *Covered Items or Information*.
3. **Export Control Risks**
4. *Nondisclosure/Confidentiality.* In most cases, proprietary/protected information provided to Rowan University under confidentiality conditions will be subject to US export controls at 48 CFR 252.225-7048 referring to Export-Controlled Items and may not be shared with foreign nationals without the approval of General Counsel and/or Division of University Research, Office of Research Compliance.
5. *Student Involvement.* Student participation on projects that require permission to publish or where results are subject to US export controls must be limited to work which is not required for the completion of their degree or program without the explicit approval of the student's Department Chair, Dean's Office and the Office of the Vice President for Research. Students have access to background proprietary information only to the extent permitted by the applicable export control regulations.
6. **Project Specific Export Authorizations**

Intended exports of *Covered Items and Information* is described below. Inclusion in this section does NOT, in and of itself, constitute approval to export; it is rather an indication to Office of Research Compliance that an export license or other authorization may be needed. This prohibition on exports includes, but is not limited to, exports to foreign nationals in the US, as well as the permanent or temporary shipment or transfer of *Covered Items and Information* out of the US.

1. **Special Clarifications**

 <Describe and detail special clarifications here>

1. **Project Personnel Requirements**

*Identification:* All students and faculty needing access to *Covered Items and Information are* identified in *Appendix 1: They will* sign an *Acknowledgement of Responsibilities*. The Responsible Person may request the addition or removal of project personnel at any time by submitting a *Revised TCP* to the Empowered Official: Dr. Mei Wei, Vice President for Research.

*Training.* All students and faculty are required to complete the University's export control training program prior to having access to *Covered Items and Information* or participating in any export controlled aspect of this project. Annual refresher training is required for all project personnel. As part of training, project personnel are made aware of what constitutes an export, their responsibilities to prevent both active and inadvertent disclosures of *Covered Items and Information*, and of the criminal and civil penalties (including prison sentences of up to 10 years and fines of up to $1M per violation) for failure to comply with US export control laws. In addition to University training requirements, students and faculty may also be required to complete any specific training required by the project leader.

S*creening*. The Division of University Research, Office of Research Compliance will screen all project personnel against the applicable lists of restricted parties and will determine the citizenship. The Division of University Research, Office of Research Compliance shall not allow project personnel access to *Covered Items and Information* until the individual has signed *Appendix 1,* completed the required training, and has been authorized by the Empowered Official.

1. **Recordkeeping**

US export control regulations require retention of records associated with all exports, use of license exceptions, and certain other activities. The Project leader shall be responsible for keeping records for the required five years from the date of the last related activity or longer if necessary to comply with regulatory requirements or the terms and conditions of the agreement with <Identify the agency/office/entity here>. Division of University Research, Office of Research Compliance will keep records pertinent to export control.

1. **End of Project Requirements**

Upon completion of this project all *Covered Items and Information* will be disposed of in accordance with applicable, Rowan University terms and US export control requirements. Hard copies will be disposed of by cross-cut shredding, incineration or return to the provider; an export license or other authorization may be required for foreign providers. Electronic files will be destroyed by using current “wiping” software. Contact Division of University Research, Office of Research Compliance and Rowan University - Information Resources & Technology for information on effective solutions for wiping. Hardware and equipment can be disposed of properly by contacting the Division of University Research, Office of Research Compliance; no *Covered Items and Information* may be added without prior approval of Division of University Research, Office of Research Compliance. This TCP must be maintained as long as *Covered Items and Information* are retained by Rowan University.

1. **Internal Notification & Assessment**

*Notification.* (1)The Project Leader shall notify the Division of University Research, Office of Research Compliance prior to adding new personnel; (2) when the scope of the project changes; (3) to request modifications to the approved TCP; and (4) when there is a change in funding, or in the award terms or conditions or change in the plan for the <Include laboratory name here> Laboratory with this TCP; or if there are any deviations from the requirements of this TCP.

1. *Certification.* The Division of University Research, Office of Research Compliance shall confirm at the beginning and end of the project to ensure that the project is being carried out in compliance with the approved TCP. This TCP must be signed at the beginning and at the end of the contracted project.
2. *Assessment.* The Division of University Research, Office of Research Compliance may conduct periodic checks and such checks may be conducted for cause or as part of a random assessment process.

TCP Prepared by: <Type in name of preparer of TCP here> Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Preparer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Director/Faculty (Lead PI/Director): <Type in name of Director/Faculty here>

Signature of Directory/Faculty:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

TCP approved by Empowered Official: <Type in name of Empowered Official>

Signature of Empowered Official: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**APPENDIX 1 - Required Personnel List**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Full Name** | **US Citizen Status** | **Signature** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |