INFORMATION AND INFRASTRUCTURE ASSURANCE

IT Security Requirements for Technology Control Plans

"Export controlled information" has been designated as one of 22 main categories of "controlled unclassified information" by the National Archives and Records Administration. The "Export Control" category of CUI includes unclassified information concerning certain items, commodities, technology, software, or other information, export of which could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. The category includes dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.

U-M Office of Research Ethics and Compliance and ITS Information and Infrastructure Assurance (IIA) have developed this guidance document to specify requirements for safeguarding U-M IT systems that maintain export controlled information.

The requirements in this document align with IT security controls described in DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012, Safeguarding Unclassified Controlled Technical Information and in NIST (National Institute for Standards and Technology) 800-171, Protecting Unclassified Information in Non-Federal Information Systems and Organizations.

These IT security requirements apply to:

- Export controlled information provided by outside parties and sponsors to the university.
- Export controlled information created at the university during the course of a project lifecycle.

Adhering to these IT security requirements is important as unauthorized disclosure of export controlled information can result in severe financial, legal, and reputational consequences for individuals and the university.

The Principal Investigator (PI) of a research project is responsible for:

- Working with the sponsor and U-M Export Control Office to determine the export controlled status of a research project.
- Working with U-M ECO and IT staff to develop a technology control plan (TCP) to safeguard any export controlled information used or generated in a research project.
- Ensuring that the research team complies with all TCP requirements for safeguarding export controlled information and with all contract or grant provisions regarding disposal of export controlled information.

A TCP must include descriptions of all of the physical and IT security measures that will be used to safeguard the electronic export controlled information used in or generated by the research. When developing IT security measures for a TCP, U-M recommends that the PI follow the guidance in this document and collaborate with department or laboratory IT manager or staff and the U-M export control office.

TCPs should address each of the following IT security measures:

Access Controls

- **Restrict access to export controlled information used in or generated by the research and to devices/systems on which that information is accessed, used, shared and stored** to only authorized project participants. Best practice is to require two barriers to access export controlled information.
    - Authorized project participants are those individuals who are listed on the technology control plan and have signed the plan and completed the export control training.
    - Account for all people—including, for example, custodial and facilities staff—that might have access to storage, office, or laboratory space where export controlled information is maintained.
- **Implement account - based access controls**. Ensure procedures are in place for issuing, altering, and revoking access privileges on shared devices and systems.
- **Implement electronic access controls.** Control access to electronic export controlled information using electronic barriers such as encryption and/or valid login credentials.
- **Implement physical access controls.** Control access to devices on which electronic export controlled information is accessed, processed or stored using physical barriers, such as a physical locks or key restrictions.
- **Avoid use of remote access.**
    - If remote access is necessary, use a secure VPN, such as the U-M VPN.
- **Do not** use personally-owned devices to access, process or store export controlled information.
- **Do not** post export controlled information to publicly available websites**.**

Storage and Transmission

- **Use secure storage services for export controlled information:**
    - If U-M ITS services will be used: Consult the Export Controlled Research (ITAR, EAR) section of the Sensitive Data Guide for guidance.
    - If computers and servers maintained by the unit or PI will be used: follow Server and Database Hardening Guides.
    - UMOR has determined that **personally-owned devices may not be used** to process, store, or access export controlled information.
    - If cloud or external service providers will be used:
        - **Whenever possible, use a vendor covered by a contract with U-M for cloud services** as listed in the Sensitive Data Guide.
        - **If a cloud vendor not covered by a contract with U-M will be used:** Document whether this is required by the grant or sponsor, verify that they can meet export control regulatory requirements related to data location and employment of U.S persons, as well as the IT security controls implemented by the vendor.
- **Avoid the use of portable storage devices such as USB drives and CDs**
    - If portable storage devices are used, they must be encrypted.
- **Use secure transmission methods for export controlled information:**
    - **Use encrypted channels** to transmit export controlled information when sending over any network.
    - If an encrypted channel is not available, ensure encryption of the file or information being shared.
    - Share export controlled information using voice or fax only when there is reasonable assurance that access to the information is limited to authorized persons only.
    - **Avoid using email** for transmitting export controlled information.

        - U-M Gmail is not approved for export controlled research.
        - Exchange Email is export control compliant.

Device Configuration and Management

Devices used to access, process, share and/or store export controlled information, such as laptops, mobile devices, and servers, should be configured according to these guidelines.

- **Configure devices to use enhanced security settings.**
    - MiWorkspace - managed devices that are identified as working with sensitive data are encrypted and provide the necessary secure system configuration for working with export controlled data.
    - University or project managed devices should be protected according to the relevant guides:
        - Servers and databases: follow Server and Database Hardening Guides.
        - Laptops and mobile devices: follow Secure Your Personal Computer.
    - UMOR has determined that **personally-owned devices may not be used** to process, store, or access export controlled information.
- **Dedicate devices for exclusive project use**. Do not use devices for both export controlled information and for general - purpose activities such as web browsing. Do not connect the devices used for export controlled information to the Internet unless required for the project.
- **Do not** take devices containing export controlled information out of the United States.
- **Do not** download export controlled information to a device when you are out of the United States.

Return and Destroy Procedures

Export controlled information must be securely disposed of once it is no longer needed.

- An appropriate TCP must remain in place as long as you retain possession of or access to export controlled information.
- When export controlled information is no longer needed, the information and any devices that contain the information must be either:
    - Returned to the original owner (grantor or sponsor), or
    - Sanitized and disposed of using secure protocols. See Secure Data Deletion and Media Disposal.
- Ensure all directives in research grants and contracts regarding return or destroy are properly followed. For some projects, NIST Guidelines for Media Sanitation may apply.
- U-M Export Control Officer will request email confirmation from the PI of the proper disposition of electronic export controlled information and associated devices at the conclusion of a project.

Traveling with Technology

- If you travel internationally in connection with your research, U.S. export control laws may apply depending on your destination and what you are taking with you.
- See the following U-M links for guidance:
    - International Center: Travel Abroad Basics
    - Office of Research Ethics and Compliance: International Travel and Export Controls
    - Safe Computing: Traveling with Technology
    - Safe Computing: Mobile Device Security When Traveling or Conducting Field Research
    - Safe Computing: Computing Guidelines for Traveling to High-Risk Locations

IT Security and Export Controls Compliance

- Everyone on the research team with access to the export controlled information must receive appropriate training about export controls and the requirements of the technology control plan.

Reporting IT Security Incidents

- **Report suspected security incidents immediately.** Suspected or actual compromises, breaches, or unauthorized disclosures of export controlled information should be immediately reported by following the instructions at Report a Security Incident. If it is determined that an export control violation occurred, the university must promptly report the violation to the contracting agency and the appropriate federal department. Examples of serious IT security incidents involving export controlled information include:
  - Unauthorized or inappropriate disclosure.
  - Suspected or actual breaches, compromises, or other unauthorized access to U-M systems, data, applications, or accounts.
  - Unauthorized changes to computers or software.
  - Lost or stolen desktop, laptop, mobile, or other data storage devices and media.

Revision History

Issued: 9/15/2016