# Guidance for the TCP Security Checklist

Use this guidance to complete the Technology Control Plan (TCP) Security Checklist.

The U-M Export Controls Program (EXP) and ITS Information Assurance (IA) have developed this guidance for safeguarding U-M IT systems and materials that maintain export-controlled information.

All U-M institutional and research data are classified into one of four classifications or sensitivity levels. **Export-controlled information is classified by U-M as High and should be protected by following the applicable minimum information security requirements for High data.** Detailed information security guidance, documentation, tools, and how-to instructions are available on the ITS Safe Computing website. U-M Information Assurance staff are available for consultation on properly securing export controlled digital environments. Request help or submit questions to IA through the ITS Service Center.

The Principal Investigator (PI) of a research project should account for the following information technology (IT) security requirements when developing a TCP. The security portion of the TCP should be completed collaboratively by the PI and the department IT manager or administrator, or other IT staff and/or IT security support staff.

In addition, all authorized research project participants with access to export-controlled information must complete appropriate security awareness training covering the following topics.

## Technology Control Plan Guidance by TCP Section

### Receipt and Transmission Security

Avoid using U-M Gmail for transmitting data **unless** Virtru encryption has been applied. U-M Gmail without the Virtru add-on is not approved for sending or receiving export-controlled information. The ITS Exchange Email is approved for export-controlled research and may be used to share research data and information with authorized persons.

### Information Security

- **Do not use personal devices when accessing export-controlled information**. The U-M Vice President for Research has determined that, under provisions of SPG 601.33, Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data, use of any personally owned device (e.g., smartphone, tablet) is prohibited for accessing export-controlled information. Only U-M managed devices are permitted for such access.
- **Avoid the use of portable or removable storage devices (e.g., USB drives, CDs) whenever possible.** If these are used for data backup, they must be encrypted, properly marked, and stored in a designated secure location with access only by authorized individuals.

## Conversational Security

- Limit project-related discussions to authorized individuals and only in areas where there is no possibility of non-authorized individuals being inadvertently included. Project-related discussions include:
    - Discussions amongst research team members of the export-controlled project,
    - Conducting tours with foreign nationals or other unauthorized individuals through research areas, and
    - Discussions with third-party vendors or subcontractors.
- **Conversations** with vendors should be conducted under the terms and conditions of signed agreements that ensure that only U.S. persons (US Citizens or US permanent residents/green card holders) are included in any conversation involving export-controlled information.

## Physical Security

- At U-M, many physical security controls are handled at the departmental, unit, or institutional level. Work with your department, unit or institutional officials to implement physical security controls for export-controlled projects.
- For those projects requiring additional physical security controls specific to a lab or other research environment, follow U-M ITS' *IT Standards for Physical Security* (DS-17); see specifically Table 1: Access and Authorization Controls and Table 2: Facility Security Controls.

## Marking or Labels for Export Controlled Materials or Information

You must mark or label export-controlled items with appropriate export control language to give notice to users. The marking/label requirement applies to export-controlled items that are kept in U-M facilities and those items that are shipped or transmitted to another location. When physical space is limited, an abbreviated marking or warning may be used.

See Markings for Export Controlled Materials and Information for guidance.

## Secure Return or Disposal of Export-Controlled Technology

- Ensure all directives in research grants and contracts regarding return or disposal of export-controlled information are followed.
- For some projects, NIST Guidelines for Media Sanitization may apply.
- For most projects responsible for handling secure deletion, follow the U-M ITS' *IT Standards for Electronic Data Disposal and Media Sanitization* (DS-11), and the specific how-to instructions found on the ITS Securely Dispose of U-M Data and Devices webpage.

# Additional TCP and Export Control Guidance

## Modifying, Extending, or Closing a TCP

Contact the U-M Export Control Program for advice on closing, modifying, or extending a TCP at the end of your research activities.

- The U-M Export Control Program will modify or extend the current TCP for any export-controlled items that you will keep after the project is closed. A TCP must remain in place with appropriate security controls until you no longer have the export control items.
- The U-M Export Control Program may close the TCP once it has determined that all export-controlled items covered by that TCP are no longer on campus or in possession of any UM employee or student.

## Reporting IT Security Incidents

**Report suspected security incidents immediately**. Suspected or actual compromises, breaches, or unauthorized disclosures of export-controlled data or materials should be immediately reported by following the instructions on the ITS Report an IT Security Incident webpage. 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 data 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

## Traveling Internationally with Export-Controlled Information

**Take precautions** when traveling internationally with export-controlled items (data, information, software).

- Traveling out of the United States with computers or other electronics containing encryption hardware or software or other export-controlled information may require an export license when traveling to certain destinations. Applying for an export license can be a very time-consuming process; consult the Export Controls Program (exportcontrols@umich.edu) well in advance of any travel that may require a license.
- Review the ITS Safe Computing While Traveling webpage for guidance.