Guidelines on Remote Access to Export Controlled Information Covered by a Technology Control Plan (TCP)

This document describes requirements for authorized faculty, staff or students who need to remotely access Export Controlled Information covered by TCPs.

When you are remotely connecting to TCP Systems\(^1\) and displaying Export Controlled Information and/or Controlled Unclassified Information “CUI” subject to NIST 800-171 controls, be aware of the potential for information to be viewed by non-authorized individuals. At no time should access to Export Controlled Information be provided to any person not explicitly authorized by the TCP. Remote access best practices include:

- **Physical controls:** Ensure that the location in which you are accessing the information is capable of preventing unauthorized access including, but not limited to the ability to close doors, blinds, etc. When participating in video conferences on platforms like Zoom and Skype ensure that Export Controlled Information is not improperly released via screen sharing or by being visible in the background.

- **Electronic controls:** Remote access to a TCP System should be made via an Ohio State owned computer or laptop that is imaged and supported by the authorized individual’s local IT Service Desk or is otherwise approved by the Office of Secure Research and your local IT. At no time should Export Controlled Information or CUI be downloaded or otherwise moved from the authorized TCP System to another device unless approved first by the Office of Secure Research and local IT.

- **Encryption:** Access to TCPs systems must be made through the university Virtual Private Network (VPN) or individual college/unit VPN. Contact your local IT Service Desk if you need access to a VPN.

These guidelines are being provided to highlight controls to help ensure that faculty, staff and students establish workflows that meet compliance guidelines stipulated in contract, university policy and required by federal regulations.

Contact the Office of Secure Research at exportcontrol@osu.edu with any questions.

---

\(^{1}\) Any device receiving, storing, processing or generating export controlled information is considered a TCP System. TCP systems must remain in locations authorized by the TCP. Contact the Office of Secure Research and your local IT to add a system to your TCP.