Guidelines on Remote Access to Controlled Unclassified Information (CUI)

Projects identified as containing Controlled Unclassified Information (CUI), have strict guidelines specified in the contract that control access to the information and auditing of access. Computer systems that store or process CUI data have a Technology Control Plan (TCP) mapping that ensures the computer is secured physically as well as electronically, based on the controls written into the contract.

Due to the workflow of many faculty and research staff in the College of Engineering, remote access to CUI information secured in an OSU office or lab is sometimes required. Guidelines are still evolving, but this document represents the current restrictions placed on authorized faculty, staff or students who need to access CUI data remotely.

Connecting to technology controlled computer systems from off-site locations and displaying CUI data has the potential for controlled information to be viewed by non-authorized individuals. At no time, will access to the CUI data be provided to any foreign person not explicitly authorized by the project TCP or by an appropriate governmental authorization. Several controls that relate to the remote access of CUI information are provided here:

- **Physical controls:** Any time an authorized individual requires remote access to a computer for the purpose of displaying CUI information, the authorized individual will ensure that the remote location they are connecting from is a facility with controls, such as doors and blinds, that prevent non-authorized individuals from observing the session.

- **Electronic controls:** Any time an authorized individual requires remote access to a computer that is a TCP controlled system, the remote device connecting to the TCP system should be an OSU owned computer or laptop that is imaged and supported by Engineering Technology Services staff.

- **Encryption:** Any time an authorized individual requires remote access to a computer that is a TCP controlled system, the connection must be made through the university Virtual Private Network (VPN).

These guidelines are being provided to authorized individuals to highlight controls required by the language in the project contract to help ensure that faculty, staff and students establish workflows that meet compliance guidelines stipulated in the project contract.