Guidelines on Using Removable Storage for Transporting 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 to ensure that are secured physically as well as electronically, based on the controls written into the contract.

Storage media includes optical media (e.g., CDs or DVDs), magnetic media (e.g., tapes or diskettes), storage devices (e.g., external drives, portable drives, or drives removed from information systems), and flash memory storage devices (e.g., USB flash drives).

If the TCP identifies that CUI will be stored on a removable storage media, devices must be handled in accordance with export regulations and CUI requirements identified by the data classification label.

- **Encryption**: Removable storage must be encrypted, to prevent data loss in the event of a lost or stolen device. Most controls call for a FIPS compliant encryption algorithm and central management of encryption keys. College of Engineering Technology Services (ETS) staff can assist in encrypting USB devices and storing security keys.

- **Labeling**: All removable storage should be labeled with the following information:

  OSU RESTRICTED DATA
  Export Classification [options: University S4 | EAR | ITAR | DFARS 7012]
  Owner: <Data owner name>

  If found, return to:
  College of Engineering
  Engineering Technology Services
  e-mail: etshelp@osu.edu
  Phone: (614) 688-2828

- **On Campus Storage**: The default policy is that when a removable storage device is not in use, it should be stored in a locked container (e.g., file cabinet, desk drawer, safe, etc.) in a room documented and approved in the TCP.

- **Transportation Off-Campus**: For projects with a TCP, if the TCP allows removable storage to be taken off-site, it should be transported in a sealed or locked container (e.g., bags or cases).

- **Chain of Custody**: If the device is transferred to another individual, the PI must record the identity of the individual the device was given to and the date on which it was given and returned. For projects with a TCP, removable storage can only be transferred to individuals explicitly authorized in the TCP.

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.