Guidelines on Purging Controlled Unclassified Information (CUI) from Windows Computers

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.

If the contract calls for data removal/destruction from computer and storage devices, specific steps must be followed to align with Defense Security Service Desktop Client Workstation Cleansing protocols.

If possible, the complete hard drive should be sanitized using a DOD approved tool for wiping storage media. Engineering Technology Services (ETS) staff have hardware and software resources that can assist with wiping media according to government regulations.

For Microsoft Windows systems, there is an approved process for purging data from a Windows storage partition without formatting the entire drive. ETS staff can assist with college managed IT devices. For self managed devices, please follow the steps below:

1. Delete all data specified for removal/destruction
2. Empty the system trash can
3. As an administrator, run the system defragmentation tool and defragment the drive
4. As an administrator, open a DOS command prompt
5. In the command prompt window, run the command
   
   cipher /w:C

   where “C” represents the drive where the data existed. If your computer has multiple drives, these steps should be run on each drive to ensure the data is completely purged from the computer.

The “cipher /w:[drive]” command will write multiple copies of zeros and ones to the free sectors of the drive, ensuring that any deleted files can no longer be retrieved.

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.