University of CINCINNATI	*Policy Title:* **Clean Desk Policy**	Policy Number: **9.1.7**
Category: Information Technology	**Effective Date:** 09/03/2021	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Faculty/ Staff/ Affiliates/ Student Workers	**Prior Effective Date:** 09/25/2019	**Responsible Office(s):** Office of Information Security

Background

To improve the security and confidentiality of university data, UC has adopted a Clean Desk Policy for workspaces. This policy reduces the risk of unauthorized access, loss and damage to information during and outside of normal business hours or when workstations are left unattended.

Policy

- Users must ensure that all Controlled Unclassified Information (CUI), Restricted or Controlled data in hardcopy or electronic form is removed from their workspace and secured in a drawer when the desk is unoccupied at the end of the workday. (See Data Governance & Classification Policy for full definitions and examples of Restricted and Controlled data).
- University owned computing device's must be session locked when not in use or when left unattended. A password must be required to unlock session lock. Kiosk, public use, interactive signage and similar devices are exempt from session locking mandate.
- Computer workstations in publicly accessible spaces must be shut down at the end of the workday, unless they need to be on to receive scheduled updates.
- Paper based file storage locations containing CUI, Restricted or Controlled information must be kept closed and locked when not in use or when left unattended.
- If left unattended in a public space, laptops, tablets and any other portable computing device must be either secured with a locking cable, locked in a drawer, secured room and encrypted.
- Printouts containing CUI, Restricted or Controlled information must be immediately removed from any shared printer.

- Restricted or Controlled documents must be shredded upon disposal. Controlled Unclassified Information must be shredded using cross-cut shredder that produces 1mm x 5mm (0.04 in. x 0.2 in.) particles or smaller, refer to NIST 800-88 for additional information.
- Whiteboards containing CUI, Restricted or Controlled data must be thoroughly erased.
- Portable electronic devices containing CUI, Restricted or Controlled data must be locked in a secure cabinet or drawer, and data must be encrypted.
- Keys used to access CUI, Restricted or Controlled data must be secured in accordance with documented university process.
- Supervisors must verify compliance with this policy through various methods including periodic walk-throughs of work areas.

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

Related Links

Data Governance & Classification Policy