University of CINCINNATI	*Policy Title:* **Clean Desk Policy**	Policy Number: **9.1.7**
Category: Information Technology	**Effective Date:** 09/25/2019	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: IT@UC	**Prior Effective Date:** 09/26/2018	**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 ensures that all sensitive and confidential information, whether on paper, storage media, or hardware is properly secured and protected from unauthorized view. 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. A Clean Desk Policy is an important security and privacy control.

Policy

- Users must ensure that all 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 work day. (See Data Governance & Classification Policy for full definitions and examples of Restricted and Controlled data). Any breach of this type of data must be reported to the Office of Information Security and the department head.
- Computer workstations must be locked when the workspace is unoccupied.
- Computer workstations must be shut down at the end of the work day, unless receiving updates during off hours.
- File cabinets containing Restricted or Controlled information must be kept closed and locked when not in use or when left unattended.
- Laptops, tablets and any other portable computing device must be either secured with a locking cable, locked in a drawer or secured room.
- Passwords may not be written down in an accessible location.
- Printouts containing Restricted or Controlled information should be immediately removed from the printer.
- Restricted or Controlled documents must be shredded upon disposal.
- Whiteboards containing Restricted or Controlled data must be thoroughly erased.
- Storage devices when not in use such as CD's, DVD, hard drives, USB drives, etc.

containing Restricted or Controlled data must be secured in a drawer and data must be encrypted.
- Keys used to access Restricted or Controlled data must be secured in a locked desk.
- 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

Definitions

Restricted data: highly sensitive data such as social security numbers, personal health information, personal identity information (PII) and financial data that must be handled with the utmost care and be protected to the greatest possible extent.

Controlled data: data such as proprietary data, graded papers, etc. which must be protected and stored securely.

Related Links

Data Governance & Classification Policy

History

Issued: 01/04/2008
Revised: 01/04/2013
Revised: 02/15/2015
Reviewed: 03/04/2016
Revised: 07/31/2016
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019