Background

To improve the security and confidentiality of information, UC has adopted a Clean Desk Policy for end user workspaces. This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access, loss of, 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 are required to ensure that any restricted and/or controlled data in hardcopy or electronic form is removed from their workspace and locked in a drawer when the desk is unoccupied and 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 IT@UC Office of Information Security and the department head.
- Computer workstations must be locked when the workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- File cabinets containing restricted or controlled information must be kept closed and locked when not in use or when not attended.
- Laptops, tablets and any other portable computing device must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing restricted or controlled information should be immediately removed from the printer.
- Upon disposal, restricted or controlled documents must be shredded.
- Whiteboards containing restricted and/or controlled data must be erased.
- Storage devices such as CD’s, DVD, hard drives, USB drives, etc. containing restricted/and or controlled data must be locked in a drawer and data must be encrypted.
- Keys used for access to restricted and/or controlled information must not be left at an unattended desk.
Contact Information

IT@UC 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.

History

Issued: 01/04/2008
Revised: 01/04/2013
Revised: 02/15/2015
Reviewed: 03/04/2016
Revised: 07/06/2016