Information Security Standard

Clear Desk and Clear Screen Standard

Initially Approved: October 17, 2016
Revised: July 14, 2020 (as the Clear Desk and Clear Screen Standard)
Revised: January 31, 2023
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This information security standard operates under University Policy 117 Information Security. A clear desk and clear screen standard reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. University Policy 97 *Information Security and Privacy Governance* requires the protection of unauthorized access to sensitive data. Additionally, much of the University's data must be protected per legal and contractual requirements.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to all University workforce members and any other person utilizing any form of University information technology or having responsibility for institutional information stored in an alternate format, such as paper.

This standard covers any papers, removable storage media and any computing devices that contain or display University information regardless of location.

III. DEFINITIONS

a. "Screen" shall mean the display portion of any computing device.

b. "Public area" shall mean a location outside of a departmental office where the public has free and easy access to the area.

c. "Secured" shall, at the very least, mean the locking of or otherwise preventing access to information, records, and/or physical space.

IV. CLEAR DESK AND CLEAR SCREEN STANDARD

The following security measures must be followed:

a. Whenever unattended or not in use, all computing devices must be left logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism (this includes laptops, tablets, smartphones and desktops). The Mobile Computing Devices Standard gives more guidance on the protection of mobile computing devices.

b. When viewing sensitive information on a screen, users should be aware of their surroundings and should ensure that third parties are not permitted to view the sensitive information.

c. Sensitive or critical business information, e.g., on paper or on electronic storage media, must be secured when not required, especially when the office is vacated at the end of the workday. The Data Handling Procedures define data sensitivity levels. The Media Handling and Disposal Standard gives more guidance on the management of removable media.

d. The creation of hardcopy material including personally identifiable information should be restricted to the minimum needed to fulfil the identified processing purpose. Paper containing sensitive or classified information must be removed from printers and faxes immediately. Faxes and printers used to print sensitive information should not be in public areas. Any time a document containing sensitive information is being printed the user must make sure they know the proper printer is chosen and go directly to the printer to retrieve the document.

e. Sensitive information on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled later and must be secured until the time that they can be shredded.

V. REVIEW

This standard will be reviewed periodically and updated as necessary.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002:2022, Clause 7 Physical Controls)
University Policy 117 Information Security
University Policy 97 Information Security and Privacy Governance
Data Handling Procedures
Media Handling and Disposal Standard
Mobile Computing Devices Standard