Clean Desk Policy

1.0 Purpose

This policy establishes the minimum requirements for maintaining a secure workspace environment, commonly referred to as a "clean desk." A clean desk practice is a critical control for protecting sensitive and confidential information (in both physical and electronic formats) from unauthorized access, disclosure, or loss. It helps reduce the risk of security breaches, increases awareness about information protection responsibilities, and supports compliance with information security standards (such as ISO 27001) and privacy regulations. The goal is to ensure that sensitive or critical information pertaining to the organization, its employees, customers, vendors, and intellectual property is appropriately secured when unattended or at the end of the workday.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and affiliates of the organization working within organizational facilities or handling organizational information assets.

3.0 Policy Statements

All individuals subject to this policy are required to adhere to the following clean desk practices:

3.1 Securing Workstations and Electronic Media

*   **Lock Workstations:** Computer workstations must be locked (e.g., using Ctrl+Alt+Del or Win+L) whenever the workspace is unoccupied, even for short periods.
*   **End-of-Day Shutdown:** Computer workstations should typically be logged off or shut down at the end of the workday, unless specific instructions are provided by IT for maintenance purposes.
*   **Secure Laptops and Portable Devices:** Laptops and other portable computing devices (e.g., tablets) must be physically secured using a locking cable or stored in a locked drawer or cabinet when unattended and at the end of the workday.
*   **Secure Removable Media:** Mass storage devices (e.g., USB drives, external hard drives, CDs, DVDs) containing sensitive or confidential information must be treated as sensitive and secured appropriately, typically by storing them in a locked drawer or cabinet when not in use.

3.2 Securing Physical Documents and Materials

*   **Clear Desks:** Sensitive or confidential documents (Restricted or Sensitive information as per the Data Classification Policy) must be removed from the desk surface and secured in a locked drawer, cabinet, or other approved secure container when the workspace is unoccupied and always at the end of the workday.
*   **Lock Cabinets:** File cabinets and drawers containing sensitive or confidential information must be kept closed and locked when not in direct use or when unattended.

*   **Secure Keys:** Keys used to access cabinets or drawers containing sensitive or confidential information must not be left unattended at a desk or in an unsecured location.
*   **Printer/Fax Output:** Printouts and faxes, especially those containing sensitive or confidential information, should be retrieved immediately from printers, copiers, and fax machines to prevent unauthorized viewing or removal.
*   **Secure Disposal:** Documents containing sensitive or confidential information must be disposed of properly using designated secure methods, such as official shredder bins or locked confidential disposal bins. They should not be placed in regular trash receptacles.
*   **Whiteboards:** Whiteboards containing sensitive or confidential information should be erased when the information is no longer needed or when the workspace will be left unattended.

3.3 Password Security

*   Passwords must never be written down and left in an accessible location, such as on sticky notes attached to monitors, under keyboards, or in unlocked drawers. Refer to the Password Policy for secure password management practices.

4.0 Compliance

4.1 Compliance Measurement

The designated authority (e.g., Precision Computer team, Facilities Security, Internal Audit) will verify compliance with this policy through various methods, including but not limited to, periodic physical walk-throughs of workspaces, awareness checks, audits, and review of security incident reports.

4.2 Exceptions

Any exception to this policy requires formal, documented justification based on business needs and must be approved in advance by the designated authority (e.g., Precision Computer team or relevant department manager). Compensating controls may be required.

4.3 Enforcement

Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures and the severity of the violation. Repeated non-compliance may lead to removal of access privileges.

5.0 Related Policies

Users should also be familiar with policies related to:

*   Data Classification Policy
*   Password Policy
*   Information Handling Policy
*   Workstation Security Policy

Revision #2
Created 28 August 2024 16:49:39 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery