Clear Desk Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company has a responsibility to maintain high standards of security for private/non-public electronic information. ABC Company data that is stored on or accessed by computers and other electronic devices must be secured against intentional or unintentional loss of confidentiality, integrity, or availability regardless of location. In addition, paper documents must also be secured and protected against unauthorized access.

# II. Purpose

This policy protects ABC Company’s assets and helps ensure our ability to continue business operations.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

The Chief Security Officer (CSO) shall ensure processes are in place to:

* Identify Sensitive Information (hardcopy and electronic) that must be protected from unauthorized access or disclosure.
* Identify workstations that must be shut down at the end of the work day vs. powered on at night so they can receive security updates.
* Laptops containing Sensitive Information must be secured per the Mobile Device Policy.

Staff shall ensure that sensitive or private/non-public electronic information is secured and removed from unauthorized disclosure or access when they leave their work areas. Staff who work with Sensitive Information should have lockable space available for storage when information is not in use. Staff must check with their immediate supervisor or Company management if an employee is not sure what information must be locked up or what lockable storage is available.

When leaving their work area, users shall ensure that their desk and work area is clear (clear desk) of papers and removable storage media. In addition, monitors shall be cleared (clear screen) to protect against unauthorized access to information or Information Systems. Screen savers shall be automatically activated after a period of inactivity. See the Workstation Security Policy for more information.

Papers and electronically stored Sensitive Information (e.g. flash drives, laptops) must be locked in a drawer when Staff leave their desks. Storage areas containing Sensitive Information must be kept locked when Staff are away from their work areas. Keys to secure storage areas must not be left in the lock or accessible by unauthorized personnel.

To prevent unauthorized disclosure or access, devices that transmit or print (e.g. Fax machines, printers) Sensitive Information shall have the documents immediately removed from the device by an authorized individual.

Documents waiting to be shredded shall not be accessible by unauthorized personnel.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.07, APO07.05, APO12.02, APO12.07, APO14.02, DSS06.07

GDPR Article 25, 32

HIPAA 64.308(a)(4)(ii)(B), 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(B)

ISO 27001 A.11.2.9

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-11, MP-2, MP-4

NIST Cybersecurity Framework ID.AM-6, ID.GV-4, ID.RA-3, PR.AC-2, PR.AT-1, DE.DP-2

PCI 9.5, 12.5.5