Workstation Hardening 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

Workstations are used by ABC Company Staff to accomplish their day-to-day duties. Workstations must be protected from both security and performance related risks. One of the required steps to attain this assurance is to ensure that the workstations are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

# II. Purpose

The purpose of this policy is to provide guidance and define the requirements for installing a new workstation in a secure manner and maintaining the security integrity of the workstation and application software.

# III. Scope

This policy applies to all Staff that use and manage ABC Company workstations.

# IV. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of information. This Policy helps ensure that access to sensitive information is restricted to authorized users.

A Workstation Hardening Procedure shall provide the detailed information required to harden ABC Company workstations. At a minimum, the Server Hardening Procedure shall include:

* Installing the operating system from an IT approved source
* Applying vendor supplied patches
* Removing unnecessary software, system services, and drivers
* Setting security parameters including workstation firewall and password at start-up
* Systems shall have a password protected screen saver activated within a short timeout period to ensure that workstations that were left unsecured are protected
* Workstations shall be protected by current and up-to-date anti-malware software and definitions

Workstations shall have vendor-issued critical security updates and patches installed in a timely manner (typically within 30 days). Refer to the Patch Management Policy for more information.

Where practical, ABC Company’s IT Department will test security patches against IT core resources before installing in production environments and rolling out to user workstations.

In the case of special applications, ABC Company’s IT Department may make hardware resources available for testing security patches.

All sensitive information must be stored on network servers. Sensitive information shall be encrypted and comply with ABC Company’s Encryption Policy. Laptops containing sensitive information shall have the hard drives encrypted and laptops shall be secured through the use of cable locks or locking laptops up in drawers or cabinets.

# 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 that use Information Resources.

**Policy History**

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

**References:**

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(7)(ii)(E)

ISO 27001:2013 6.1.3, 8.3, A.13.1.1, A.14

NIST SP 800-37 3.3, 3.4

NIST SP 800-53 AC-3, AC-17-18, AC-20, PL-2, PL-7-8, SC-7-8, SC-10

NIST Cybersecurity Framework ID.AM-6, ID.RM-1, PR.AC-5, PR.DS-1-2, DE.CM-1

PCI 2.1-3, 2.5-6, 4.1, 5.1