Workstation Hardening Procedure

|  |  |
| --- | --- |
| 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

Policies provide management direction and guidance to ensure systems and data are properly protected. Procedures document a detailed description of the steps necessary to perform specific operations that comply with ABC Company’s policies.

# II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in ABC Company's Workstation Hardening Policy.

# III. Scope

This procedure applies to IT Department Staff who administer workstations.

# IV. Procedure

Physical security. Ensure workstations are placed in physical locations that restrict access to authorized individuals. Laptops and other mobile devices shall be secured through the use of cable locks or locking the devices in drawers or cabinets when not in use.

Accounts. Delete unneeded user accounts.

Applications. Remove unneeded programs, applications, and services.

Alerts, advisories, and vulnerability announcements. Monitor manufacturer alerts, advisories, and vulnerability announcements. Ensure patches and updates are installed at the time a new workstation is placed into production and on-going per the Patch Management Policy.

Passwords. Educate users to choose a long and complex memorized secret (i.e. password) that complies with the Password Policy. When changing a password, educate users not to choose a recent prior password (password history). See the Password Policy for more information.

Groups. Where possible, assign the user/account to a group. Review and maintain group access rights on a regular basis.

Firewall. As a general rule, each workstation should have a software firewall activated on the device. The software firewall helps protect against network based attacks.

Anti-Malware. Ensure the device is protected from malicious software such as viruses, worms, Trojan Horse programs, etc. Ensure the Malware software and definitions are updated in a timely manner. Refer to the Anti-Malware Policy for more information.

Sharing. Where possible, disable file and printer sharing services.

Monitors. Configure workstations to have a password protected screen saver activated within a short timeout period. This ensures that workstations that were left unsecured are protected. Position monitors so that only authorized personnel can read the information on the screen.

Data. Where possible, configure the Workstation so all Sensitive Information is 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.

Testing. Where possible, the device should be tested prior to installing the device in a production environment.

Management sessions. Administrators should not connect to the device using unsecure services where communications are not encrypted. Ensure only authorized personnel are allowed to access and administer the device.

Manufacturer resources. Refer to manufacturer resources for additional guidance on hardening workstations and specific security functionality.

# V. Enforcement

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

# VI. Distribution

This procedure is to be distributed to IT Department Staff who administer workstations and the Chief Security Officer.

**Procedure History**

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