Workstation Security 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

This document describes a required minimal security configuration for all workstations connected to a production network or used in a production capacity at or on behalf of ABC Company.

# II. Purpose

The purpose of this policy is to ensure the security of ABC Company Information Systems, workstations, and data.

# III. Scope

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

# IV. Policy

This Policy helps ensure that access to sensitive information is restricted to authorized users. By following appropriate security measures, Staff can help ensure information integrity, confidentiality, and availability.

Staff shall follow appropriate guidelines and procedures when using workstations and systems. ABC Company has implemented certain technical, physical, and administrative controls and safeguards to ensure that workstations restrict access to authorized users

Physical access to workstations shall be restricted to only authorized personnel. Staff shall prevent unauthorized viewing of information on a screen:

* Staff shall ensure that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to prevent public viewing.
* Staff shall manually activate a password protected screen saver when they leave their desk.
* Systems shall have a password protected screen saver activated within a short timeout period to ensure that workstations that were left unsecured are protected.

Prior to leaving for the day, staff shall:

* Exit running applications and close any open documents.
* Ensure workstations are left on but logged off in order to facilitate after hours updates.

Staff shall comply with all applicable policies and procedures including:

* Acceptable Use Policy
* Anti-Malware Policy
* Mobile Device Policy
* Password Policy
* Remote Access Policy
* Wireless Access Policy

Staff shall use workstations for authorized business purposes only and only approved personnel may install pre-approved software on workstations.

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.

The IT Department shall ensure that all workstations use a surge protector (not just a power strip) or a UPS battery backup. Staff shall keep food and drink away from workstations in order to avoid accidental spills.

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

Workstations shall have active and updated anti-malware protection software. Staff shall not disable anti-malware protection software. See Anti-Malware Policy for more information.

Each workstation shall have an active software firewall that protects the device from external threats. Staff shall not disable the firewall.

# 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)(5)(ii)(B), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)

ISO 27001:2013 8.3, A.6.2, A.11.2, A.12.2, A.12.6

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-7(2), AC-11, AC-17, AC-18, AC-19, AT-2, MP-2, MP-4, SI-3, SI-4(24)

NIST Cybersecurity Framework ID.RA-6, PR.AC-2, PR.DS-3, PR.IP-5, DE.CM-1, RS.RP-1

PCI 1.4, 2.1, 6.2, 9.1