Hardware and Software Maintenance 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

Maintenance of Information Resources hardware and software is part of ABC Company’s risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

# II. Purpose

The formal process of maintaining hardware and software ensures that a clearly defined set of procedures is used to document and minimize risks related to Information Systems.

# III. Scope

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

# IV. Policy

This policy identifies the hardware and software maintenance and support arrangements for all standard and non-standard Information Resource servers, network infrastructure equipment, workstations, peripherals, and related software. This policy includes applications and systems that are subject to their own maintenance and upgrade policies. The IT Department will ensure that hardware and software maintenance activities are properly recorded in the Information Systems Log Form.

A. Hardware

The IT Department will:

* Ensure that important servers and network infrastructure are covered by on-site warranty agreements from the appropriate vendors with a response time sufficient to meet business needs.
* Arrange for faulty items that are under warranty to be repaired.
* Arrange for repairs or replacement of equipment that is not covered by warranty.

The IT Department will procure and install other types of network and computer hardware including printers, scanners, monitors, keyboards, mice, etc. This ensures:

* The equipment is compatible with existing ABC Company equipment.
* Centralizes purchasing so the best price is received.
* Equipment is under warranty and maintenance support agreements.
* The equipment is properly configured and has security controls.

B. Software

For the purposes of this Policy, software includes:

* Operating systems, virtualization, firmware, and related software.
* Major applications such as order processing, customer relationship management, HR, E-mail, etc. and related databases and interfaces
* Office productivity software including spreadsheets, word processing, presentation, etc.
* Third party applications such as Internet browsers, Adobe Acrobat Reader, media players, Flash Player, etc.
* Security protection software such as firewalls, anti-malware, etc.
* Utilities and other tools

The IT Department shall be responsible for the installation and maintenance of software. The IT Department shall:

* Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry accepted definitions. Update system configuration standards as new vulnerabilities are identified.
* Install and maintain software.
* Maintain software license records.
* Fully test the application and ensure it is compatible with and runs on IT Department standard hardware.
* Where appropriate, subscribe to vendor software maintenance.
* Ensure the software is configured to run at optimum levels.
* Ensure the software and data are fully backed up to ensure systems can be recovered in the event of a failure.
* Updated with critical system patches within 30 days of release. Patches are to be tested before rolling out to production environments.
* Ensure third party vendors work in conjunction with the IT Department.

C. Approval

All departments must seek approval from the IT Department prior to purchasing any special or non-standard hardware, software, or other equipment. IT Department support for non-standard hardware, software, or other equipment will be assessed and agreed on a department-by-department basis.

# V. Enforcement

Any Staff member 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 APO01.03, APO09.05, APO10.05, APO11.09, APO13.07, BAI02.05, BAI04.05, DSS04.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(e)(2)(i), 164.314(a)(2)(i)

ISO 27001:2013 4.4, A.11.2.4, A.15.2.1, A.17.1.2

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 MA-2, MA-6

NIST Cybersecurity Framework ID.RA-4, ID.RA-6, PR.AC-2, PR.MA-1, PR.MA-2, DE.DP-2

PCI 8.1, 8.3.2, 9.7, 9.9.3