Patch Management 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 policy identifies the need to apply vendor-issued critical security updates and patches regularly to protect ABC Company data and systems. It applies to all electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, mobile devices, Smartphones, etc.

# II. Purpose

Software is critical to the delivery of services to ABC Company’s customers, Staff, and business partners. 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

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. The latest stable version of any security related updates shall be installed on all network devices. System components and devices attached to the network must be regularly maintained including the application of critical security patches within 30 days after release by the vendor. Other patches not designated as critical by the vendor must be applied on a normal maintenance schedule, which may depart from the above. Note: Critical security patches should be identified according to a risk ranking process.

After testing software patches and updates, automated software update tools shall be used, where possible, to ensure that operating system and third-party software applications are running the most recent security updates provided by the vendor. Many vendors have automated the patching procedure, particularly for desktop computers. While there is some potential for error by the vendor, the risks are substantially less than if patches are never applied at all due to oversight.

Patches on production systems (e.g. servers) may require complex testing and installation procedures. In certain cases, risk mitigation, rather than patching, may be preferable. The risk mitigation alternative selected should be in proportion to the risk. The reason for any departure from the above standard and alternative protection measures taken must be documented in writing for devices storing non-public data.

The regular application of critical security patches is reviewed as part of the normal ABC Company audit procedures.

Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.

Patching should include updates to operating systems as well as office productivity software, data base software, third party applications (e.g. Flash, pdf, etc.), and mobile devices with access to ABC Company Information Resources.

# 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 IT Staff.

**Policy History**

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

**References:**

COBIT APO05.03, APO05.05, APO11.09-10, BAI06.02, BAI06.05-06, BAI07.06, BAI10.07

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.310(c)

ISO 27001:2013 A.11.2.4, A.11.2.6, A.12.1.2, A.12.6

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 RA-3, RA-5, SI-2, SI-5

NIST Cybersecurity Framework ID.RA-2, ID.RA-6, ID.RM-1, PR.IP-3, DE.DP-2

PCI 6.1, 6.2