Patch Management 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

This procedure ensures important vendor-issued security updates and patches are applied in a timely manner.

# 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 Patch Management Policy.

# III. Scope

This procedure applies to all Staff responsible for patching and updating of ABC Company Information Resources.

# IV. Procedure

System components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. The latest stable version of any security related updates is installed on all network devices. System components and devices attached to the network are 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 are applied on a normal maintenance schedule, which may depart from the above. Critical security patches are classified according to a risk ranking process.

After testing software patches and updates, automated software update tools are used, where possible, to ensure that operating system and third-party software applications are running the most recent security updates provided by the vendor.

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

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

Application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner. A risk-based approach is used to prioritize critical patches.

Patching includes 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 procedure may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This procedure is to be distributed to all ABC Company IT Staff responsible for patching and updating of Information Resources.

**Procedure History**

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