**XYZ Company Patch Management Policy**

**Overview**

XYZ Company is required to mitigate patch risk for the confidentiality, integrity, and availability of XYZ systems.

Utilizing patch management defends against vulnerabilities associated with critical infrastructure to maintain the XYZ security posture.

XYZ Company is to ensure the acquisition and monitoring of devices through patch management. Moreover, XYZ Company will discover flaws in critical infrastructure to enforce patches on all devices.

**Purpose / Scope**

The purpose of this document is to identify system vulnerabilities and software issues that disrupt normal operations of the XYZ Company. The incorporation of patches is to assist individuals within the XYZ Company for adopting software security control measures throughout the organization.

The scope pertains to recommendations for aligning the IT department with XYZ business mission and operations. The IT department will be prepared to update patching techniques for workstations as necessary.

**Responsibility**

It is the duty of the IT department head to provide a secure work environment in the XYZ Company. Servers, laptops, desktops, virtual machines, peripherals, and network components will be analyzed for patching under the IT department head.

All IT department employees are responsible for carrying out patches on the analyzed devices. In addition, all employees are to maintain workstations associated with each device.

**Software Inventory**

The following inventory lists software in need of patching:

| **Software** | **S-ID** |
| --- | --- |
| Microsoft Excel | 1001 |
| Norton Antivirus | 1002 |
| XYZ Web Server | 1003 |
| XYZ VPN | 1004 |
| CRM Software | 1005 |
| Adobe | 1006 |

**Routine Patching**

Regular patching with backups is recommended for maintaining the XYZ Company’s security posture. All routine patching will occur every Monday of the following week to reduce delays in emergency patching.

**Vulnerability Deadline**

| Importance |  |  |  |
| --- | --- | --- | --- |
|  | Low | Medium | High |
| Critical | 58.7 days | 23.7 days | 3.6 days |
| High | 66.8 days | 32.9 days | 7.2 days |
| Medium | 76.5 days | 41.4 days | 10.5 days |
| Low | 89.6 days | 49.3 days | 13.4 days |

**Software Maintenance**

* Prepare and deploy software updates regularly
* Enforce vulnerability correction for the identified issues
* Incorporate disclosure best practices with incident response
* Test patching before deployment to ensure minimal disruptions
* Provide lessons learned to mitigate similar issues in the future