# System Update Policy

## Overview

Regular system updates and patching provides a mechanism for [LEP] to manage and protect hardware and software from security and functional issues. System updates can take the form of firmware, software, or physical hardware updates relevant to any vulnerabilities in a particular piece of hardware, software or system appliance.

## Purpose

This policy establishes a minimum process for protecting assets and employees from security vulnerabilities. This policy provides procedures and supports for how updates are to be performed for all hardware and software.

## Scope

This policy applies to all [LEP] staff, users, and contractors that create, deploy, or support information technology within the [LEP].

## Policy

This policy defines methods and procedures used to determine what updates should be applied and timing of the updates. The following areas shall be monitored and addressed when performing system updates.

### **UPDATE MONITORING**

Several types of system updates shall be monitored from hardware and software perspectives:

* BIOS, Firmware, and other component flash memory in appliances and computers
* Operating systems and key management utilities
* Productivity and application software updates
* Miscellaneous utility software updates (e.g. Flash, Adobe Reader)

[LEP] support staff shall use the following mechanisms to assess requirements and the necessity for [LEP] hardware and software updates:

* Review of posted security flaws and patches for each type of hardware and software updates applicable to the system. These reviews include industry alerts, vendor notifications, or security threat notifications. If automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.
* Automatic scanning to determine available updates and patch status of the system or application.

The [Insert Appropriate Role] or their designee shall develop procedures to:

* Determine appropriate patch or configuration changes for systems and applications. Updates shall be checked no less than weekly to determine whether any new updates are required.
* Manage a regular patching and update schedule [LEP]-wide that ensures all appropriate hardware, appliances, and software is checked for functional and security updates.
* Ensure that patch and configuration change management works as designed and desired without causing other disruptions. Where possible, a test environment shall be used to validate and assess patch viability in the pre-production environment.
* Prioritize and schedule updates and patches.
* Maintain logs of machine patching and schedules. Logs shall be electronic wherever appropriate and possible.
* Execute appropriate [LEP]-wide communication and change management when patching systems.

### **UPDATE PREPARATION**

[LEP] systems personnel shall do requisite research and testing prior to applying updates. In general, the following should be well understood before approving and applying updates:

* The addressed vulnerability
* Previous patches or required system updates
* Programs affected by the change
* Problems that may result as a result of the change
* Procedures to back out or undo the change

In addition, the [Insert Appropriate Role] or their designee shall ensure that:

* All patches approved for [LEP] systems are logged prior to their production release. Logging may be managed at the [Insert Appropriate Role]’s discretion.
* New patches shall be tested in a controlled test environment that mimics the production infrastructure before they are applied. This is mandatory for enterprise applications and services where outage would cause significant organizational or customer impact.
* Staff shall ensure that backups exist of applications and data prior to installing a patch or update. Each server shall have documentation that identifies the list of applications running on the device and a patch history.

### **APPLYING UPDATES**

System-wide updates shall be performed on a schedule approved by the [Insert Appropriate Role] or their designee. Patching of systems shall be rotational and follow a regular, documented and communicated schedule. The following procedures apply to all update processes:

* Updates may be performed manually, using administrative tools, or automatically using vendor or internally provided vehicles.
* All workstations and user systems/application (as applicable) shall have current operating system and application versions. These systems shall be patched on a regular basis as established by management.
* Server and enterprise application updates shall be performed by a qualified and authorized system administrator after the update has been tested in a non-production environment. Assuming software compatibility, servers shall have current versions of the operating systems and associated If automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Suitable audit documentation and controls may include:

* Historical change management documentation as it applies to patch management processes, procedures, and protocols
* Archival logs of completed patching cycles
* Evidence of ongoing compliance with patching procedures including test environments, correspondence, and other procedural components

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all staff involved in management and patching of [LEP] systems.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 12/07/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |