# Software and Firmware Patch Management Policy

## Overview

Software is critical to the delivery of services to [LEP] customers, staff, and partners. Software patching provides a mechanism to regularly update features and protect software with current enhancements and bug fixes. This policy is designed to protect [LEP] users and assets from potential functional, security, and malware breaches and helps ensure business continuity and operations across the enterprise.

## Purpose

Regularly applied vendor and internal firmware and software updates/patches help to protect [LEP] software, data, and systems. This policy applies to all electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, mobile devices, smartphones, building control and security systems.

## Scope

This policy applies to all [LEP] staff that create, manage, deploy, or support application and system software or devices within the [LEP]. It covers [LEP]-wide firmware, system, application, and utility software patching procedures.

## Policy

All hardware and software system components shall be protected from known vulnerabilities by managing and applying regular procedures for installing applicable system and application security patches.

System components and devices attached to the [LEP] network must be regularly maintained including the application of critical security and functional patches within a reasonable timeframe (no more than 45 days) allowing for testing and deployment after release by the vendor. Other patches designated as non-critical by the vendor or [LEP] management must be applied on a regular and normal maintenance schedule as defined by [LEP] information systems personnel.

Many vendors have automated patching procedures and tools. Using these automated tools lowers risks substantially from manual patching processes.

It is understood that that patches on production systems (e.g. servers) may require complex testing and installation procedures prior to installation. In certain cases, risk mitigation rather than patching may be advisable. A mitigation selection alternative should be considered in proportion to the risk. [LEP] requires that departures from the above standard and alternative protection measures taken be documented in writing for devices storing non-public data.

Policies and procedures shall be established and delivery mechanisms implemented for vulnerability and patch management. These procedures shall ensure that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner taking a risk-based approach for prioritizing critical patches. The regular application of critical security patches shall be reviewed as part of normal operating procedures. These procedures shall be implemented through a change/configuration management meeting process specified through [LEP] management.

Patching shall include:

* Firmware and hardware specific components
* Updates to operating systems and office productivity software
* Application and data base software
* Third party applications, application software
* Mobile devices with access to [LEP] resources

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal application development and release methodology. Management controls include:

* Regular and documented [LEP] change management meeting where patch and configuration management is discussed, prioritized and scheduled for release
* Automated patch management on a regular schedule with [LEP] approved software that carries logs of changes applied
* Documentation of policy exception and risk mitigation

## 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 [LEP] staff responsible for maintenance, support, and enhancement of systems and applications.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 09/09/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |