# Hardware and Software Maintenance Policy

## Overview

Maintenance of hardware and software assets is part of a comprehensive management process to minimize disruptions, optimize costs, provide asset stewardship, and bring best practice to the organization. Effective maintenance and support of assets provides longer life, higher employee productivity, and increased user satisfaction.

## Purpose

The formal process of maintaining hardware and software ensures that a clearly defined set of procedures is used to manage system resources. [LEP] has a substantial investment in hardware, software, network devices, and peripherals. Proper maintenance and support of these assets increases usability and lowers the total cost of ownership to the organization. This policy is designed to support preventative and ongoing maintenance of [LEP] computer and software assets.

## **Scope**

This policy applies to all [LEP] staff that support and maintain computer hardware and software for the organization.

## Policy

### **General**

Hardware and software maintenance and support arrangements shall be required for all standard and non-standard desktop, servers, network infrastructure equipment, peripherals, and related software. This shall include applications and systems that are subject to their own proprietary maintenance and upgrade policies. Service, maintenance and support shall be properly staffed and managed through a ticket management system and help desk.

### **B. Computer and Network Hardware**

[LEP] management and the [LEP] Helpdesk shall ensure:

* All infrastructure desktop, servers, peripherals and network hardware (switches, routers, firewalls) are covered by on-site warranty agreements with appropriate response times to meet business continuity needs
* Defective items under warranty are repaired in a timely fashion
* Repairs or surplus of equipment not covered under current warranty meet all state and [LEP] protocols and procedures

The [LEP] [Insert Appropriate Department] under the direction of [Insert Appropriate Role] shall centrally procure and install all network and departmental computer hardware including but not limited to desktops, servers, audio-visual, security, laptops, printers, scanners, monitors, keyboards, and mice. This shall ensure:

* The equipment is compatible with existing [LEP] hardware standards and software
* Hardware and software standards are enforced
* Centralized purchasing supplies the best price for goods
* Equipment is covered under appropriate warranty and maintenance support agreements
* Configuration management and security policy implementation are consistent and minimize organizational risks
* The equipment is properly configured and has appropriate security controls/software

### **D. System and Application Software**

For the purposes of this policy, computer software shall include:

* Operating systems, virtualization, firmware, and related software
* Major applications such as general financials and ERP, student information systems, learning management systems, email, and related databases/interfaces
* Office productivity software including spreadsheets, word processing, presentation, etc.
* Third party utility and productivity applications such as Internet browsers, Adobe Acrobat Reader, media players, Flash Player, etc.
* Security protection software such as firewalls, anti-malware, etc.
* Utilities and other tools

IT support shall be responsible for the installation and maintenance of all [LEP] software. IT support under the direction of the [Insert Appropriate Role] shall:

* Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry accepted definitions
* Periodically update system configuration standards as new vulnerabilities are identified
* Install and maintain system and end-user software
* Maintain appropriate software license records for compliance purposes
* Fully test applications to ensure they are compatible with and run on standard [LEP] hardware
* Subscribe to vendor software maintenance programs where appropriate and applicable
* Tune and analyze operational software configurations for optimum performance
* Ensure software and user data are fully backed up in the event of a failure
* Update critical system patches within 30 days of release
* Patches shall be tested before deployment to production environments
* Ensure third party vendors and contractors work in conjunction with the [Insert Appropriate Department, Group, or Role] and uphold all [LEP] policies and procedures

Individuals seeking exceptions to this policy must seek approval from [LEP] management and the [Insert Appropriate Role] **PRIOR** to purchasing any specialized, non-standard hardware, software, or equipment. Support for non-standard hardware, software, or other equipment shall be assessed and agreed upon on a case-by case basis by [LEP] management.  
  
5. Audit Controls and ManagementOn-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal processes and procedures. Example audit control and management evidence includes:

* Documented hardware and software standards with evidence of regular review and update
* Asset and software management and tracking systems and tools
* Hardware and software configuration standards, tools, and orderly system builds
* Exception logs for user standards hardware/software deviation
* Regular and operational demonstration of patch, change and configuration management processes and procedures/notifications

## 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 and contractors using [LEP] information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/26/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |