# Server Hardening Policy

## Overview

Servers in their many forms (file, print, application, web, and database) are used by the organization to supply critical information for staff. These assets must be protected from both security and performance related risks. One of the required steps to attain this goal is to ensure that hardware (whether on premise or in the cloud) is installed and maintained in a manner that prevents unauthorized access, unauthorized use, consistent configuration, and minimal service disruptions.

## Purpose

Appropriate measures must be taken when configuring and managing server based resources to ensure the confidentiality, integrity and availability of information. This policy provides general procedures and requirements for installing server based resources in a secure manner as well as maintaining the security integrity of the hardware and application software.

## III. Scope

This policy applies to all [LEP] staff that use, deploy, or support [LEP] server hardware/virtual resources.

## IV. Policy

### General

A server hardening procedure shall be created and maintained that provides detailed information required to configure and harden [LEP] servers whether on premise or in the cloud. The procedure shall include:

* Installing the operating system from an IT approved source
* Applying all appropriate vendor supplied security patches and firmware updates
* Removing unnecessary software, system services, protocols, ports, and drivers
* Setting security and operational parameters including configuring system services, firewall, anti-virus, anti-malware, and local system passwords/accounts
* Enabling appropriate local file system/sharing permissions, audit logging, local/physical security, reporting, and intrusion detection software as applicable
* Applying [LEP] Domain-based Active Directory server based group policy

### Operations and Maintenance

[LEP] server support shall perform the following procedures and processes to ensure hardening compliance after the initial system is delivered:

* Post-Install operating system, utility/system service patches (e.g. COM and .NET), database, web, and application security patches shall be pre-tested and deployed on a regular basis against similar systems before rolling out to the production environment.
* In the case of custom applications or enterprise software, [LEP] server support shall take appropriate precautions to ensure patch compatibility prior to install. Should a patch be incompatible with a specialized software package, exceptions must be approved in writing by the [Insert Appropriate Role] or their designee.
* All sensitive information shall be encrypted at-rest and in-transit as well as complying with the [LEP] Data Encryption Policy. Where appropriate, PKI certificates/key strategies shall be used to additionally secure web based access.
* Periodic audits of server compliance shall be conducted at least annually. Results shall be documented and any deficiencies corrected.

## 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 processes and procedures. Examples of appropriate controls and documentation are:

* Documented server build processes and images
* Internal configuration and asset management protocols and procedures
* Patch logs containing server name, patch installed, service installed and date
* GPO documentation showing hardening and security measures employed across the enterprise
* Archival audit documentation with results and remedies taken to address security concerns

## 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 using, supporting, and configuring desktop workstations.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/16/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |