# 3.7 - Maintenance

### Control Satisfaction Matrix

| Standard | Category | Controls Satisfied | 800-53r4 Controls | ISO/SEC 27001 | Audit Controls |
|---|---|---|---|---|---|
| NIST 800-171 | Maintenance | 3.7.1 - 3.7.6 | MA-2, MA-3, MA-3(1), MA-3(2), MA-4, MA-5 | A.11.2.4, A.11.2.5 | 19.0 |

#### Major Document History

| Date | Comment | Who |
|---|---|---|
| 5/13/2019 | Initial Doc | Tharp |
| 6/03/2019 | Added Control Objectives, Assertions, Actions | Tharp |
| 6/21/2019 | CO's & Assertions updated with feedback from B&V CPA's | Tharp |
| 7/30/2019 | Added 19.0 | Tharp |
| 7/30/2019 | Strike thru control Objectives | Tharp |
| 8/12/2019 | Formatting Updates | Tharp |
| 8/29/2019 | Copied Content For IS-1 SOC submission | Tharp |
| 10/6/2021 | Policy's Reviewed for Audit | Tharp |

---

## Purpose and Scope

The purpose of this policy is to set at a minimum systems maintenance standards. If a higher standard is practical DLZP Group will adopt the highest maintenance standards

## Background

All DLZP built infrastructure for IT systems labs and client hosted environments are built with code within Amazon Web Services. This code provides repeatability and efficiency to design, build and maintain these systems. This code may be highly optimized and automated through the adoption of one or more services to monitor, secure and manage this infrastructure.

## Policy

### 3.7.1

Regular Maintenance shall be performed on to the extent possible based on the class of IT systems managed e.g. IaaS, PaaS.

### 3.7.2

Processes be they automated or manual shall be scripted and followed each for each maintenance period. For automated maintenance logging or alerts will be relied upon to validate maintenance. A technical and program lead shall be assigned to all hosted systems.

### 3.7.3

Out of Scope

### 3.7.4

Diagnostic Tests and Services must be scrutinized to ensure they don't harbor or introduce malicious code into the maintained environment.

### 3.7.5

All DLZP Systems are remote and maintenance activities must integrate with existing identify and access policies. If appropriate maintenance scoped ID's should be used to provide a separation of duties from other support activities.

### 3.7.6

No maintenance will be performed by unauthorized staff or vendors.

---

# Response Plan

# 19.0 Patch Management and Systems Update Plan

## 19.1 Patch Management Overview

Patches are usually released for three reasons:

1) To fix faults in an application or operating system.

2) To alter functionality or to address a new security threat.

3) To change or modify the software configuration to make it less susceptible to attacks and more secure.

This Plan establishes a patch management and systems update Plan for all IT systems, devices and appliances, regardless of operating system or platform.

## 19.2 Plan

DLZP has established and implemented an automated company-wide system of patch management for all IT systems, devices and appliances, regardless of operating system or platform. This consists of clearly assigned specific responsibilities for the Systems Administrator. All authorized personnel are trained in system administration to include patch management techniques. Patch management is used in conjunction with the normal vulnerability scanning efforts. DLZP may use automated patch management software to keep patches current, and certifies that system patches have been applied using appropriate logging methods. These logs and reports will be completed on an ongoing basis and kept on file for audit and/or review.

Patches are tested on non-production systems prior to installation on all production systems. In addition, DLZP maintains an organizational systems and software inventory and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to external entities.

## 19.3 Plan Exception Requirements

Exceptions to Plan will be considered only in terms of implementation timeframes - exceptions will not be granted to the requirement to conform to this Plan. Exceptions that are approved will be interim in nature. Interim exceptions cannot extend beyond the fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. The System Administrator will monitor all approved exceptions.

## 19.4 Procedures

Although the National Institute of Standards and Technology (NIST) recommends that companies establish a “Patch and Vulnerability Group”, this is optional in establishing a patch management program. DLZP has established a program utilizing the most efficient and effective way to manage patches possible given their environment. At a minimum, the following duties and responsibilities have been delegated to the System Administrator:

### 19.4.1 Create and Maintain an Organizational Systems and Software Inventory to include a Patch Management Database containing:

- Hardware equipment and software packages
- Version numbers of those packages within the organization
- Patches that apply to this equipment and patch status.

Most automated patch management programs provide this functionality and are preferred over manual patch solutions. This database enables the Systems Administrator to monitor for information about vulnerabilities and patches that correspond to the hardware and software within the inventory. Specific attention is given to those software packages that are used on important servers or that are used by a large number of systems. This includes any connected resources and

any external resources that are used for official DLZP business. This database is updated in a timely manner when a system is installed or upgraded. Post-patch distribution updates to the database are executed immediately following any patching exercise.

### 19.4.2 Identify Newly Discovered Vulnerabilities and Security Patches

The Systems Administrator is responsible for proactively monitoring security sources for vulnerabilities and patches that correspond to the software within the organizational hardware and software inventory. A variety of sources are monitored to ensure that they are aware of all the newly discovered vulnerabilities. When a vulnerability has no satisfactory patch, the Systems Administrator presents alternative risk mitigation approaches to management and supports that management decision by testing, documenting, and coordinating implementation with the appropriate system. Most automated solutions will perform the bulk of this requirement; any devices not covered by the automated system will be recorded manually in the database.

### 19.4.3 Prioritize Patch Application

The Systems Administrator prioritizes the set of known patches. The criticality of a patch is a risk-based decision utilizing standard elements such as Probability and Consequence. Consideration of consequences usually extends beyond a system’s logical boundaries and requires a broader approach in weighing this factor. For example, DLZP will always consider Operating System (OS) Patches that are deemed critical by the software vendor as critical. A distinction is made between servers and end-user systems when making patching recommendations because often it is more important to patch servers on a routine schedule before end-user systems. Care is taken to ensure that the automatic patch distribution solution targets the correct machines. Patches deemed critical are tested and installed on applicable systems within calendar 30 days of general release. Engineering patches (i.e. beta service packs) are generally avoided unless the criticality is extremely high and the general availability release date poses a significant risk to the target systems.

### 19.4.4 Identify Patches and Vulnerabilities Associated with Software On Local Systems

As previously mentioned, the organizational software inventory and patch database may not contain all software used by DLZP. All patches applied or vulnerabilities identified will require correction and testing in accordance with the procedures outlined above.

## 19.5 Corporate Responsibilities

#### 19.5.1 The President

- Supports the establishment and maintenance of patch management Plan and procedures within DLZP
- Ensures that funding and personnel are provided to effectively maintain enterprise-wide patch management solutions

#### 19.5.2 The Systems Administrator

- Develops and publishes Plan and procedural guidance on patch management
- Provides enterprise-wide tools to assist in compliance efforts

- Monitors patch management on an enterprise-wide basis
- Provides advice and guidance in effectively patching systems and eliminating vulnerabilities
- Supports exception requests from the patch management Plan to ensure that appropriate security protection is provided
- Implements an internal program for patch management on all IT systems
- Ensures that all IT professionals are trained and made aware of this Plan
- Clearly assigns authorized personnel specific patch management and vulnerability correction responsibilities
- Employs an approved automated patch management solution to facilitate compliance with this Plan and to promote efficiency for all systems, and applies patch management solutions to in-house applications and monitors the status of those systems
- Reports patch management status monthly
- Requests a formal exception through the established process for any systems which are not compliant within 90 days
- Stays current with new patch management Plan, procedures, and enterprise wide solutions
- Acts as a Point of Contact (POC) for security to provide guidance and assistance to any individuals designated patch management responsibilities

---