

# 

# 

**Patch Management Policy**

|  |  |
| --- | --- |
| Number: | IOPS-POL-0001 |
| Business Unit: | Infrastructure Operations |
| Owner: | Matthew Horowitz |
| Email: | Matthew.Horowitz@msg.com |
| Written by: | Adrienne D Myers, MS, CISSP |
| Go Live Date: | [Publish Date] |

# Foreword

This document describes the policy requirements for maintaining up-to-date operating system security patches on all Madison Square Garden Company-owned and managed servers.

**Contents**

[Foreword 0](#_Toc25330112)

[1 Purpose and Goals 2](#_Toc25330113)

[1.1 Abstract 2](#_Toc25330114)

[1.2 Audience 2](#_Toc25330116)

[1.3 Scope 2](#_Toc25330118)

[2 Policy 3](#_Toc25330120)

[3 Roles and Responsibilities 3](#_Toc25330121)

[3.1 The Maintenance procedures include the following tasks: 3](#_Toc25330122)

[3.2 The Responsible Parties are as follows: 3](#_Toc25330123)

[3.3 RACI Diagram 4](#_Toc25330124)

[4 Deployment Activities 4](#_Toc25330125)

[5 Change Management 4](#_Toc25330126)

[6 Monitoring and Reporting 5](#_Toc25330127)

[7 Enforcement 5](#_Toc25330128)

[8 Exceptions 5](#_Toc25330129)

[9 Definitions 5](#_Toc25330130)

[10 Review and Approval 6](#_Toc25330131)

# Purpose and Goals

## Abstract

## MSG Infrastructure and Information Security is responsible for ensuring the confidentiality, integrity, and availability of MSG data, and that of customer data stored on its systems. MSG Infrastructure Engineering has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

## Audience

## This document is intended for all MSG system administrators and technical staff, including IT Services staff who are responsible for the ongoing maintenance of MSG services and systems. Potential consumers of this document also extend to be anyone else who is similarly undertaking activities governed by this policy.

## Scope

## This policy applies to servers owned or managed by MSG. This includes systems that contain company or customer data owned or managed by MSG regardless of location. The following systems have been categorized according to management:

Table - Servers and Responsible Groups

|  |  |
| --- | --- |
| Server Type | Responsible Group |
| QA/PS Production | Venue Application Team |
| Dev, QA/PS, Production | Business Systems |
| Production | Infrastructure Operations |
| Production | Network Operations |
| QA/PS, Production | IT Service Management |
| Production | Creative Services |
| Production | Other |

# 

# Policy

Servers owned by MSG must have up-to-date (as defined by tenable.io minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. These minimum baseline requirements are produced to guide IT Administrators in mitigating known vulnerabilities based on Common Vulnerabilities and Exposures (CVE) and Knowledge Base (KB) data mapped to specific operating systems. This policy helps to ensure the security of the MSG asset and the data that resides on MSG systems. Any exception to the policy must be documented and forwarded to the Infrastructure Operations Director for review. See Section 6 on Exceptions.

# Roles and Responsibilities

The Maintenance procedures include the following tasks:

* Testing patches on Dev/QA/PS servers
* Confirmation of Dev/QA/PS application functionality post-test patch deployment
* Deployment of patches to production servers
* Confirmation of production application functionality post-patch deployment
* Periodic vulnerability scanning of network systems

## The Responsible Parties are as follows:

* **Information Security Office**: Performs nightly vulnerability scan of MSG servers using tenable.io application. Produces and distributes reports to System Operations Team (servers). Informs System Operation Team of Critical and High Zero-day Out-of-Band Patches that must be applied immediately.
* **System Operations**: This team approves and deploys the monthly patches in ManageEngine Patch Manager plus cloud. The System Operation Team ensures that MSG servers patching is kept up to date. The Team uses both ManageEngine Patch Manager plus cloud and tenable.io reports provided by ISO to accomplish patch deployment activities.
* **Application Owners**: This group provides a desired patching window for their servers. This group ensures that the System Operation team is informed of any exceptions to patching associated with their servers.

RACI Diagram

Table - RACI Diagram

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| **Approving Server Patch Window** | App Owner | App Owner | Application Team(s) | System Operations Team |
| **Review Monthly Security and Zero Day Patches** | ISO | ISO | Vendors | System Operations Team |
| **Approving Server Patches** | System Operations Team | System Operations Team | Vendors | ISO |
| **Testing Server Patches** | System Operations Team  Application Team(s) | System Operations Team  Application Team(s) | Application Team(s) | Application Owner  IT Infrastructure Engineering Director |
| **Patching** | System Operations Team | System Operations Team | Application Team(s) | Application Owner  IT Infrastructure Engineering Director |

# Deployment Activities

Critical and High-Security Patches must be deployed within 30 days of release. Medium and Low-Security Patches must be deployed within 90 days of release. This is in accordance with Requirement 6 of the PCI-DSS and PCI-DSS Attestation compliance.

Non-production (Dev, QA/PS server) patching can be deployed outside of standard maintenance window(s) upon agreement with the Application Owner. After deployment of non-production patches, the Application Owner must test their application and report the results of testing back to the Systems Operations Team within five (5) business days.

Production patching must be applied in accordance with the standard maintenance windows. The Application Owner must report back the results of production application testing to System Operations 24 hours of production patch deployment.

# Change Management

Change Management is only applicable to the deployment of patches on production servers. Prior to patch deployment a ServiceNow change request (CR) shall be submitted by the System Operations Team. The ServiceNow CR must be approved by the Application Owner, the IT Infrastructure Operations Director, and the Vice President of IT Service Management. The Change request should specify pertinent details regarding the server(s) to be patched.

# Monitoring and Reporting

The System Operations Team will produce patch deployment status reports as a post-patch deployment activity.

# Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees at MSG Systems Engineering. Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action.

# Exceptions

When an exception to the formal patching policy is required a written request for exception must be submitted to the IT Infrastructure Engineering Director. Any servers that do not comply with policy must have an approved exception on file with the IT Infrastructure Engineering Director. Please refer to theIT Infrastructure Engineering Director or representative for details on filing exceptions.

# Definitions

Table - Definition of Terms

|  |  |
| --- | --- |
| Term | Definition |
| Patch | A piece of software designed to fix problems with or update a computer program or its supporting data |
| Trojan | A class of computer threat (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions |
| Virus | A computer program that can replicate itself and infect a computer without the permission or knowledge of the owner. |
| Worm | A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth. |
| ISO | Information Security Office |
| PCI-DSS | Payment Card Industry - Data Security Standard |
| Dev | A server that facilitates the development and testing of programs, websites, software, and applications for software developers. |
| QA/PS | A Quality Assurance / Production Support Server that facilitates the measurement of the quality of software/hardware. A staging or pre-production server. |
| CVE | Common Vulnerabilities and Exposure – a list of entries of publicly known cybersecurity vulnerabilities. <http://cve.mitre.org> |
| KB | A knowledge base is a database used for knowledge sharing and management. Numerous vendors publish knowledge bases e.g. Microsoft, Oracle, etcetera. |

# Review and Approval

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Name | Title | Signature | | Date | |
| Author | Adrienne D Myers, MS, CISSP | Technical Writer | Adrienne D Myers | | November 15, 2019 | |
| Reviewer | Adriano Sverko | Peer Reviewer | Adriano Sverko | | November 15, 2019 | |
| Authorizer |  | Director |  | |  | |
|  |  |  |  | |  | |
|  |  |  |  | |  | |
| Contributors | | | | | | | |
| Claude Vilfort, System Administrator | |  | Adriano Sverko, Technical Writer | | | |
| Anthony Ray, System Administrator | |  | Victor Leung, Security Architect | | | |
| Nick D’Angelo, System Administrator | |  |  | | | |
|  |  |  |  | |  | |
|  |  |  |  | |  | |
| Revision History | | | | | | | |
| Version | **Date** | **Writer** | **Notes** | | | |
| FINAL DRAFT | November 22, 2019 | Adrienne Myers |  | | | |
|  |  |  |  | | | |
|  |  |  |  | | | |
|  |  |  |  | | | |
|  |  |  |  | | | |
|  |  |  |  | | | |
|  |  |  |  | | | |
|  | | | | **Effective Date** | | **Review Date** | |
|  | |  | |