**Patch Management Policy and Procedure**

Doc ID /POL/0.1

Document Classification: Internal

July 2022

**Document Control**

| Document Name | Patch Management Policy and Procedure |
| --- | --- |
| Document ID | POL/0.1 |
| Security Classification | Internal |

| **Authorization** | | |
| --- | --- | --- |
| Document Owner | Reviewed by | Authorized by |
|  |  |  |

| **Amendment Log** | | | | |
| --- | --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Section** | **A/M/D** | **Brief description of the change** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**TABLE OF CONTENTS**

red1.0 Overview 4

2.0 Purpose 4

3.0 Scope 4

4.0 Roles and Responsibilities 4

5.0 Policy 5

5.1 Security Patch Management Program Employee 6

5.2 Asset Inventory 6

5.3 Industry Leading Software Sources and Additional Supporting Resources 6

5.4 Risk Ranking for Security Patch Management 6

5.5 Database of Remediation Activities that need to be applied 7

5.6 Test Procedures for Testing Patches Regarding Remediation 7

5.7 Distribution, Deployment and Implementation of Patches and other Security-Hardening Procedures 7

5.8 Verifying Successful Implementation of Patches and other Security-Hardening Procedures 8

6.0 Procedures 8

7.0 Process 8

7.1 End-users Computers 8

7.2 IT Servers and Network Devices 8

7.3 Production 8

7.4 Zero Day and Emergency Security Patching 8

8.0 Responsibility for Policy and Procedures Maintenance 9

9.0 References 9

# Overview

One of the most critical initiatives for ensuring the confidentiality, integrity and availability (CIA) of any organization information systems environment is that of comprehensive security and patch management procedures. Cyber Security threats are posing serious challenges for many IT professionals, as attackers and malicious exploits are constantly seeking to penetrate vulnerabilities within ones’ network architecture. Having critical systems resources operating without the latest security updates poses a serious danger to their safety and security, which in turn can results in these systems being severely compromised. Being proactive and having a well-defined patch management framework – one with documented policies and procedures in place – is what’s needed for every organization today, regardless of industry, size or location.

As for patch management itself, from an information security perspective, it is best defined as the following:

“The policies, procedures and related processes undertaken for effectively identifying, acquiring, testing, distributing, installing and monitoring security patches for all relevant system resources throughout a {Conpany}’s, including, but not limited to, all network devices, operating systems, applications, and other in-scope systems.”

In accordance with mandated {Conpany} security requirements set forth and approved by management, {Conpany} has established a formal patch management policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on an annual basis for ensuring its adequacy and relevancy regarding {Conpany}’s needs and goals.

# Purpose

This policy and applicable supporting procedures are designed to provide {Conpany} with a documented and formalized process for acquiring, testing, distributing, installing and monitoring security patches. Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity and availability of {Conpany}’s system components.

# Scope

This policy and supporting procedures encompass all system components that are owned, operated, maintained, and controlled by {Conpany} and all other system components, both internally and externally, that interact with these systems.

* Internal system components are those owned, operated, maintained and controlled by {Conpany} and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.
* External system components are those owned, operated, maintained and controlled by any entity other than {Conpany}, but for which such external resources may impact the confidentiality, integrity and availability (CIA) and overall security of the aforementioned description of “internal system components”.
* Note: While {Conpany} does not have the ability to actually provision, harden, secure and deploy another {Conpany}’s system components, {Conpany} will follow best practices as required by obtaining all relevant information ensuring that such systems are safe and secure.

# Roles and Responsibilities

Implementing and adhering to {Conpany} all policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees and users of system components, along with vendors, contractors and other relevant third parties. Additionally, by being aware of one’s roles and responsibilities as it pertains to {Conpany} information systems, all relevant parties are helping promote the confidentiality, integrity and availability (CIA) principles for information security in today’s world of growing cyber security challenges.

* **Management Commitment**: Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Management Representative is to report to other members of senior management on a regular basis regarding aspects of the {Conpany}’s information systems posture.
* **Internal Employees and Users**: Responsibilities include adhering to the {Conpany}’s information security policies, procedures, practices, and not undertaking any measure to alter such standards on any {Conpany} system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day to day operations – may also notice issues that could impede the safety and security of {Conpany} system components and are to also report such instance immediately to senior authorities.
* **Vendors, Contractors and Third-Party Entities**: Responsibilities for such individuals and organization are much like those stated for end users: adhering to the {Conpany}’s information security policies, procedures, practices and not undertaking any measure to alter such standards on any such system components.

# Policy

{Conpany} needs to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated {Conpany} all security requirements set forth and approved by the management.

In accordance with best practices for security patch management, the subsequent three security concerns will be highlighted throughout the patch management policy and procedures. They are as follows:

**Vulnerabilities:** Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the environment or any other IT resources.

**Remediation:** The three primary methods of remediation are: installation of a software patch, adjustment of a configuration setting and removal of affected software.

**Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses and Trojan horses.

Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments. This includes but not limited to the following:

* Network devices and all supporting hardware and protocols.
* Operating systems within the development and production environments.
* Applications within the development and production environments.
* Any other mission-critical resources within the environment that require patches and security updates for daily operations.

Additionally, a Security Patch Management Program is to be implemented, which consists of the following initiatives:

* A formalized Security Patch Management Program employee, complete with his / her roles and responsibilities.
* Comprehensive inventory of all system components and IT resources.
* Subscribing to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues.
* Procedures for establishing a risk ranking regarding security patch management. This will include but is not limited to the significance of the threat, the existence and overall threat of the exploitation and the risks involved in applying security patch management procedures (its effect on other systems, resources available and resource constraints).
* The creation of database of remediation activities that needs to be applied.
* Test procedures for testing patches regarding remediation.
* Procedures for the deployment, distribution and implementation of patches and other related security hardening procedures.
* Procedures for verifying successful implementation of patches and other related security-hardening procedures.
* Installation of applicable critical vendor-supplied security patches within one month of release.
* Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

## Security Patch Management Program Employee

This individual(s) will be responsible for coordinating, facilitating and undertaking all necessary activities regarding security patch management policies and procedures. Additionally, this individual(s) will have the necessary information technology and security expertise to successfully execute all steps as required. Specifically, this individual(s) will have a strong working knowledge of vulnerability and patch management, as well as system administration, intrusion detection and firewall management.

## Asset Inventory

Asset Inventory includes all system components which includes, but not limited to, information assets, software assets, physical assets and any other components as needed.

## Industry Leading Software Sources and Additional Supporting Resources

Various external security sources and resources are utilized to ensure that {Conpany} maintains awareness of security threats, vulnerabilities and what respective patches, security upgrades and protocols are available.

Currently, {Conpany} subscribes to the following types of security sources and resources:

* Vendor websites and email alerts
* Vendor mailing lists, newsletter and additional support channels for patches and security
* Third-party websites and email alerts
* Third-party mailing lists
* Online forums and discussion panels
* Conferences, seminars and trade shows

Refer to vendor list for specific security resources and sources to which {Conpany} subscribes for patch management, alerts, security and support as applicable.

## Risk Ranking for Security Patch Management

A Risk Ranking matrix will be established regarding security patch management. Specifically, system components and other associated IT resources will be given a risk ranking pertaining to the importance of security patch management activities to be undertaken.

{Conpany} will adhere to the following definitions regarding risks that are related to all system components within the environment and any other IT resources:

**High:** The threat source is highly motivated and sufficiently capable; controls to prevent the vulnerability from being exercised are ineffective.

**Medium:** The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

**Low:** The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Additionally, the Security Management Program employee will also be responsible for the following critical activities:

* Being aware of all known threats or vulnerabilities that could significantly impact system components within the environment and any other IT resources. This requires consistent oversight and management of all online resources used for security patch management.
* Having a strong technical and business understanding of all critical systems within the {Conpany}’s IT infrastructure, as well as knowing which systems are essential for day-to-day operations.
* Having response mechanisms and procedures in place to immediately report the scope of the exploitation (systems affected), the impact to the IT infrastructure as a whole and which remediation activities and plan of action initiatives are already available to the management in the event of network exploitation.

## Database of Remediation Activities that need to be applied

The database for remediation activities will consist of listing the relevant Uniform Resource Locations (URL) for each patch and specific advice and any other comments deemed critical to the patch itself. Additionally, the Security Patch Management Program employee will be responsible for keeping the database accurate and relevant.

## Test Procedures for Testing Patches Regarding Remediation

Security patch management testing procedures must be observed to ensure the authenticity of the patch or any other security upgrades before they are released to day-to-day operations.

The following testing procedures are to be adhered to:

* An acceptable test environment (non-production systems) will be determined and utilized, if necessary, for each and every patch and security upgrade implemented by the Security Patch Management Program employee.
* For vendors providing patches, the authenticity of the downloaded patch will need to be verified. This verification process will be determined as needed for patches and security upgrades.
* A virus scan is to be run on all patches before installation.
* Determine patch dependency and any other issues that may result in the installation of the patch. Would the installation of the new patch disable another? Are other patches uninstalled when the new patch is installed?

## Distribution, Deployment and Implementation of Patches and other Security-Hardening Procedures

All patches and security updates are to be pushed out in a formalized and secure manner, with all critical patches installed within one month of release from a vendor or other approved third party. This includes using the following:

* Enterprise Patch Management Software
* Secured email lists sent to authorized personnel
* Secure internal web source for retrieving patches sent out by the Security Patch Management Program employee

## Verifying Successful Implementation of Patches and other Security-Hardening Procedures

It is the responsibility of the Security Patch Management Program employee to verify the successful implementation of all patches and security upgrades to {Conpany}’s IT infrastructure. These activities will consist of, but are not limited to, the following:

* Verifying that the files have been changed as stated in the vendor’s documentation to reflect the updates as needed.
* Verifying whether the recommended patches and security updates were installed properly by reviewing patch logs.

# Procedures

{Conpany} is to ensure that all applicable users adhere to the following procedures and supporting activities listed below. Additionally, the relevant procedures will be fully enforced by {Conpany} for ensuring such initiatives are executed in a formal manner and on a consistent basis for all specified systems resources.

* Undertake all necessary activities for ensuring the aforementioned policies are implemented. This ultimately requires coordination amongst various {Conpany} personnel, along with utilizing various security tools, vendor documentation, and other supporting materials for ensuring the stated policy mandates are met.
* Update the Asset Register, Vendor List as per the defined frequency.
* If changes must be made to system components – such as additional hardening procedures, configuration changes, or any other necessary IT changes for ensuring continued compliance with the aforementioned policies – then a ticket / change order is to be opened and submitted in the ticketing tool / service desk which effectively details the reason for the change, what actual changes will be done, why, and any other relevant information.

# Process

## End-users Computers

* Scan for available patches
* Download necessary patches from a trusted source (as made available)
* Schedule Deployment
* Deploy patches

## IT Servers and Network Devices

* Scan for available patches
* Download necessary patches from a trusted source (as made available)
* Deploy Patches
* Verify Services
* Notify and Report Testing Results

## Production

* Patches are deployed and applied
* Create a service desk ticket one week before the maintenance date
* Deploy patches
* Communicate extended outages to appropriate teams. If outages goes past window, IT must communicate it to the respective stakeholders
* Verify services

## Zero Day and Emergency Security Patching

* The IT team shall determine the risk and the relevance of the patch, as well as when the system can be patched
* Create a service desk request before the maintenance date
* Notify the users
* Deploy patches
* Verify services
* Notify and report testing results

# Responsibility for Policy and Procedures Maintenance

Management Representative is responsible for ensuring that the aforementioned policy initiatives, and if applicable – relevant procedures – are kept current as needed for purposes of compliance with mandated {Conpany} all security requirements set forth and approved by management.

# References

* Asset Register
* Vendor List