Patch Management Policy

**Version 1.0**

< Date>

|  |
| --- |
| **History Log****Date****Author** |
| **Version** | **Date** | **Author** |
|  |   |  |
|  |  |  |
|  |  |  |

Contents

[1. Goal 3](#_Toc118047937)

[2. Scope 3](#_Toc118047938)

[3. Policy General Provisions 3](#_Toc118047939)

[3.1 Responsibility 3](#_Toc118047940)

[3.2 Patch Management Preparation Process 3](#_Toc118047941)

[3.3 The Update Process 4](#_Toc118047942)

[3.4 The Update Schedule 4](#_Toc118047943)

[3.5 Request for Update 5](#_Toc118047944)

[3.6 Updating Test Environment of the System 5](#_Toc118047945)

[3.7 Updating of the Prod Environment of the System 6](#_Toc118047946)

[3.8 Actions Against Zero Day Vulnerabilities 6](#_Toc118047947)

# Goal

The goal of this patch management policy (hereinafter, “the Policy”) is to strengthen the company's information security by keeping the Systems as up to date as possible and to minimize maintenance errors in order to minimize the likelihood of malicious actors successfully using exploits to attack the company. The Policy is also intended to ensure the smooth operation of the Systems.

This Policy is to assist in providing direction, establishing goals, enforcing governance, and to outline compliance.

# Scope

The Policy defines the process for updating and storing versions of all test and production information systems (hereinafter, “the Systems”). This Policy applies to all computing devices connected to the <Name of the Organization> network (including but not limited to Personal Computers, Servers, Main Frames, Software, Databases, PDAs, and Notebooks etc.)

# Policy General Provisions

Patch Management is to Protect <**Name of the Organization**> Systems from vulnerabilities in a timely manner to maintain systems stability and enhance systems functionalities to optimum performance at all times.

## 3.1 Responsibility

Representatives of the CyberSecurity (CS) department are responsible for updating the Systems. This work is to be performed in conjunction with the Information Technology (IT) department. Every user, both individually and within the organization, is responsible for ensuring prudent and responsible use of computing and network resources.

## 3.2 Patch Management Preparation Process

* All information related to patches is to be downloaded from authorized/trusted sources.
* CS department is to subscribe to mailing list of Vendor or reputable outside security agencies e.g. OWASP, NIST, CIS, CERT etc. to receive the security vulnerabilities/zero-day vulnerabilities and new patch release notifications related to all system platforms and software used in organizational environment
* CS department is to perform the security impact review for each of the new security vulnerability discovered and assign the risk ranking (for example ‘High’, ‘Medium’ & ‘Low’). CS department can follow any of the below approach to determine the vulnerability risk ranking:
	+ CVSS base scores of vulnerabilities
	+ Vendor / OEM defined risk ranking for vulnerability
	+ Vulnerability scanning tool, defined risk ranking for vulnerability
* CS department must consider likelihood and exploitation factor for the vulnerabilities to decide the risk and risk ranking

## 3.3 The Update Process

The update process includes:

* Identifying all software, information, objects, databases, and hardware in the Systems that require updates
* Identifying the core stakeholders for each System
* Identifying maintenance days for each System
* Obtaining formal approval from the System stakeholders before starting the update process
* Gaining temporary, least-privileged access to each target System to perform its updates
* Gaining authorization from the System owner for updates in the test environment
* Checking the test environment’s availability and functionality after the update, and rolling back the changes if something goes wrong
* Gaining authorization from the System owner for updates in the production environment
* Checking the production environment’s availability and functionality after the update, and rolling back the changes if something goes wrong
* Monitoring the update process
* Ensuring that the System’s technical documentation is revised after each update

## 3.4 The Update Schedule

* + Applicable Critical vendor-supplied security patches shall be installed within one month from release to all the systems in <**Name of the Organization**> IT environment and prioritized based on the severity and impact of vulnerabilities
	+ IT operations shall maintain a published schedule for deploying patches
	+ Ensure that all system components and software have the latest vendor-supplied patches installed. Only relevant patches must be installed as per the schedule defined below (exception: virus outbreak and similar situations)

|  |  |
| --- | --- |
| **Patch Category** | **Patch Deployment Schedule** |
| System Critical Patches (Higher Risk) | Within 24 Hours to 1 Month (based on severity) |
| System Non-Critical Patches (Lower Risk) | 1 Month to 6 months  |

## 3.5 Request for Update

* Update requests are submitted electronically by the CS department in the project management system. The request must include:
	+ The name of the update officer from the CS department
	+ The name of the System and its owner
	+ The name of the update operator from the IT department
	+ Date of test environment update
	+ Date of production environment update
	+ Update details and purpose
	+ Possible system downtime time period
	+ Brief technical description of the update
* Each update request is recorded in the project management system.
* The update must be approved by the Systems owner.
* The update request is assigned to the responsible IT department.
* The CS department must keep an update control log that registers update requests and tracks the status of requests.

## 3.6 Updating Test Environment of the System

* The CS department sends the update package or a link to the updates to the IT department via the project management system.
* Updating of the test environment of the System is performed by the IT department in cooperation with the CS department at the scheduled date and time.
* Representatives of the IT department check that the test System works as intended:
	+ If the test environment of the System is updated successfully, the update is recorded in the project management system.
	+ If problems are found, they are recorded in detail along with how critical they are. The CS department and the System owner analyze this information, assesses the risk, and determines whether to install the update in the production environment and records the decision and reasoning in the project management system.
* After the release of a new software version, the IT department checks the update again in the test environment to exclude new errors and records the results in the project management system.
* The System owner acknowledges the conclusion of the test environment update.

## 3.7 Updating of the Prod Environment of the System

After functionality verification in the test environment and approval of the System owner, the IT department finalizes the upgrade plan for the production environment.

* The plan details the date of upgrade, its duration, participants, and the list of recipients to be notified.
* The plan is coordinated with the CS department and the System owner.
* After approval of the plan by the IT department, an announcement of the unavailability of the System and planned work shall be sent by email to all System users at least 24 hours in advance.
* The IT department updates the prod environment of the System in the presence of the System owners.
* The IT department and the System owner check that the System works as intended. If problems are found, the System owner decides how critical they are to the operation and approves a rollback if needed.
* The IT department records the results in the project management system, and notifies the CS department.

## 3.8 Actions Against Zero Day Vulnerabilities

When patches are not readily available, or their deployment has unacceptable adverse impacts on business, operations teams must consider the following mitigating controls for risk management:

* + Network filtering.
	+ Increased monitoring.
	+ Awareness training / communications.
	+ Temporarily disabling impacted services / features.

This policy was approved by TITLE and is issued on a version-controlled basis under his/her signature

Signature: Date: