**Vulnerability Management Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_fqowhy6wyx2g) **4**

[**Scope**](#_w78n5sz7w0qv) **4**

[**Policy**](#_2pj7zc7tszf) **4**

[**Vulnerability Scan Targets**](#_pdotlv14u4on) **4**

[**Vulnerability Scan Scope and Frequency**](#_qx97ssmefyr7) **4**

[**Vulnerability Scanning**](#_xodhwnbqere8) **5**

[**Vulnerability scan of the customer-related environment workflow**](#_t4qn46dmtk2l) **5**

[**Patch Management**](#_dgwd69t0bcyx) **5**

[**Vulnerability Severity**](#_kmrlenc026w7) **5**

[**Vulnerability Remediation**](#_lo492u9yyhq7) **6**

[**Vulnerability Remediation Terms**](#_gfjhc6g701gv) **6**

[**Rescan**](#_sx5mxa48oybf) **6**

[**Change, Review, and Update**](#_w1o88vxspwq8) **6**

[**Disciplinary Action**](#_mm5ewidk84i8) **6**

[**Responsibility**](#_kyzyjwcjae82) **7**

[**Related Documents**](#_5fmzdjr161kx) **7**

# 

# **Purpose**

The purpose of this policy is to define the requirements for notification, testing, and installation of security-related patches on devices and EC2.

# **Scope**

This policy applies to all *[Company]’s* electronic devices and resources, including computer workstations, servers, etc.

# **Policy**

* All devices shall be scanned on a consistent scan schedule and also on a by-request or as-needed basis.

## **Vulnerability Scan Targets**

| System/Application | Description |
| --- | --- |
|  |  |
|  |
|  |
|  |
|  |  |
|  |
|  |  |

## **Vulnerability Scan Scope and Frequency**

Below are listed the vulnerability scan tools used per software component, and per item is listed how frequent these are performed.

| **Scan Target** | **Scan Frequency** |
| --- | --- |
|  |  |
|  |
|  |  |
|  |  |
|  |  |

## **Vulnerability Scanning**

* This procedure applies to AWS infrastructure, which is used for providing service for *[Company]’s* customers. **Quarterly** configuration scans are performed to detect vulnerabilities in the customer-related environment.

### **Vulnerability scan of the customer-related environment workflow**

* The assigned person performs the vulnerability scan.
* The report with detected and assessed vulnerabilities is generated after the scan, and the Jira ticket is closed with the report as evidence.
* If any new vulnerabilities are found, then:
  + The Jira ticket is created for the detected vulnerabilities.
  + Detected vulnerabilities should be added as child issues into Jira ticket(s) and assigned to IT Operations Engineer(s), who will be responsible for implementation remediation actions.

## **Patch Management**

### **Vulnerability Severity**

* **Critical** - Imminent security risk due to vulnerability has to be resolved immediately.
* **High** - Potential substantial security risk due to vulnerability has to be as soon as possible.
* **Medium** - Nature of vulnerability or impact of it is not seen as an immediate security risk. It has to be resolved in a defined time.
* **Low** - Vulnerability poses no direct security impact so that it can be postponed to mitigate more high-severity vulnerabilities found.

### **Vulnerability Remediation**

* The severity of the findings is evaluated according to the given report.
* DevOps team executes the remediation plan in line with the agreed deadlines.
* Any occurred problems during the implementation must be recorded and further analyzed. Alternative actions should be defined and tested.
* IT Manager then validates the remediation plan to be completed.

### **Vulnerability Remediation Terms**

| **Target** | **Critical** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- | --- |
| Application Servers | Immediate | One week | Three weeks | Two months |
| Staff Devices | One day | Two weeks | Two months | Six months |
| Bamboo | Immediate | One week | Three weeks | Two months |

## **Rescan**

* Once a vulnerability is remediated, a rescan must be scheduled to verify the remediating actions have been implemented.
* This scan will be performed using the same vulnerability scanning tools and identical configuration settings as the initial scan.
* Typically, a rescan is scheduled after the deadline for implementing remediating actions.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

IT Manager is responsible for assessing and applying security patches that impact systems under their management and supervision.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Change Management and Control Policy