©(ORGANISATION NAME)

PATCH MANAGEMENT POLICY

Subject: Patch Management Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 8	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 INTRODUCTION

Patch management is the process of applying updates to software, drivers, and firmware to protect against vulnerabilities. Effective patch management also helps ensure the best operating performance of systems, boosting productivity, thereby protecting the origination from potential breaches on confidentiality, integrity, and availability.

Reference	Description of Risk
SAFETag	Patch & Vulnerability Management on BYOD and Office Devices
SAFETag	Vulnerability Scanning and Analysis
SAFETag	Vulnerability Research

1.1 OBJECTIVE

The objective of the patch management policy is to minimise the Organisation's exposure to security threats through effective management of its network, systems, application, and database vulnerabilities.

1.2 POLICY STATEMENTS

1.2.1 The Organisation shall task and equip a team/individual saddled with the responsibility of patch testing and deployment, vulnerability mitigation and remediation, incident containment and eradication.

1.2.2 The Organisation shall task a team/individual (with the Information Technology/ Security) with the vulnerability assessment of its infrastructure (Application, Database, Network and Systems).

1.2.3 The team/individual tasked with the responsibility of patch management shall perform all relevant assessments (including regulatory; where required) and generate or obtain the corresponding clean reports; this assessment should be conducted on a quarterly basis at the minimum.

1.2.4 The team/individual tasked with the responsibility of patch management shall draw up a schedule of routine scans targeted at improving the Organisation's security posture; the team shall perform the scan based on their schedule and obtain applicable evidence of remediation from the relevant stakeholder(s).

1.2.5 The team/individual tasked with the responsibility of patch management shall perform a vulnerability assessment of its applicable systems once there is a major change within the IT environment.

1.2.6 The team/individual tasked with the responsibility of patch management shall see to the annual performance of penetration test on the Organisation's IT infrastructure; where there is unavailability or resources within the Organisation, a Third-Party Organisation or competent external resource shall handle the penetration test. The penetration test shall include Network Layer, Application Layer, Database Layer, Web Servers, People and Physical Layer.

1.2.7 The team/individual tasked with the responsibility of patch management shall assess the Organisation's wireless access points and ensure non-susceptibility to known wireless network vulnerabilities and exploitation techniques.

1.2.8 The Organisation shall equip the team/individual tasked with the responsibility of patch management with tools capable of effectively monitoring and reporting on the Organisation's IT infrastructure.

1.2.9 The team/individual tasked with the responsibility of patch management shall monitor the Organisation's IT infrastructure and report (when applicable) on confirmed incidents and suspected Indicators of Compromises (IoCs).

1.2.10 The team/individual tasked with the responsibility of patch management shall categorise all identified vulnerabilities based on impact; the Organisation shall adopt the vulnerability categorization below:

- **Critical**: These are vulnerabilities whose impact could adversely affect or bring to a halt, the Organisation's business operations if exploited.
- **High:** These are vulnerabilities whose impact could disrupt the Organisation's business operation if exploited.
- **Medium**: These are vulnerabilities whose impact is marginal on the Organisation's business operation.
- **Low/Informational**: These vulnerabilities do not directly affect the Organisation's business operation.

1.2.11 The team/individual tasked with the responsibility of patch management shall execute a risk assessment of identified vulnerabilities for which recommended fixes are not feasible; the team shall put in place compensating controls and share the outcome of their risk assessment with the relevant stakeholders (i.e. CIO/CISO/Head of IT, or as specified).

1.2.12 Staff shall not make any temporary changes to information systems for the sole purpose of "passing" an assessment; the Staff's Disciplinary Committee shall handle identified cases of temporary system adjustment described above.

1.2.13 The team/individual tasked with the responsibility of patch management shall test all patches prior to deployment to the production environment.

1.2.14 The team/individual tasked with the responsibility of patch management shall balance security with business objectives; the team shall assess the impact of scans and schedule scans for periods of minimal impact on the Organisation's services and infrastructure.

1.2.15 Technology shall ensure no interference between the approved scanning tools and the target systems; scanning tools must be able to scan target systems without hindrances.

1.2.16 The team/individual tasked with the responsibility of patch management shall ensure the testing and deployment of critical security patches during the immediate maintenance window succeeding the patch release date.

1.2.17 The Head of Internal Audit (or any other specified internal assurance stakeholder i.e., Head of Internal Control) shall independently audit the Organisation's vulnerability management process; the audit shall focus on determining the effectiveness of the vulnerability management process in place within the Organisation.

2.0 PATCH MANAGEMENT SCHEDULE

Patching Schedule depicts the agreed and documented plan detailing the policy and procedure for implementing software patches.

2.1 SERVICE LEVEL AGREEMENT FOR TIME TO PATCH

This depicts the acceptable threshold for applying patches based on the categorization of the patch.

SN	PATCH CATEGORY	DESCRIPTION	TIME TO PATCH
1	Critical	● Patches that have a rating of CVSS rating of 9.0 to 10.0 ● Patches that are considered mandatory by the vendor. ● Patches released to address vulnerability exploit that is known to have occurred. ● Patches that address any vulnerability that should be prioritised for immediate remediation	1 to 10 Days of discovery
2	High	● Patches that have a rating of CVSS rating of 7.0 to 8.9 ● Patches that address any vulnerability that should be reviewed and remedied wherever possible.	11 to 45 Days of discovery
3	Medium	● Patches that have a rating of CVSS rating of 4.0 to 6.9 ● Patches that address any vulnerability that pose minimal risk to data security.	46 to 90 Days of discovery
4	Low	● Patches that have a rating of CVSS rating of 1.0 to 3.9 ● Patches that address any vulnerability that are cautionary or informational in nature	90 to 180 Days of discovery

2.2 GOVERNANCE ON PATCH MANAGEMENT

2.2.1 The team/individual tasked with the responsibility of patch management shall on a periodical basis (weekly/monthly/quarterly) render the patch management report to the relevant stakeholders (i.e. CIO/CISO/Head of IT, or as specified). The report shall not be limited to the following:

- Scan report for vulnerable systems or systems identified with missing patches.
- Report of the applied patches
- Current status of the patches applied to the systems.

2.2.2 The Organisation shall task an independent assurance team/individual (Internal Control, Compliance, or Internal Audit) to conduct a routine review to evaluate the level of compliance with the patch management policy.

3.0 RECOMMENDATIONS/ADVISORY ON PATCH MANAGEMENT

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff

• Consider the use of windows update for prompt patch management. https://support.microsoft.com/en-us/windows/update-windows-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a • Consider the use of MacBook update for prompt patch management. https://support.apple.com/en-ng/108382	• Consider the use of windows update for prompt patch management. https://support.microsoft.com/en-us/windows/update-windows-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a • Consider the use of MacBook update for prompt patch management. https://support.apple.com/en-ng/108382 • Consider the use of open-source patch management solutions i.e. https://www.pdq.com/pdq-deploy/ https://opsi.org/en/	• Consider the use of open-source patch management solutions i.e. https://www.pdq.com/pdq-deploy/ https://opsi.org/en/ • Consider the use of enterprise/proprietary patch management solutions. https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-endpoint-configuration-manager https://www.hcl-software.com/bigfix • Consider the use of Mobile Device Manager i.e. https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune