|  |
| --- |
| Wise Digital Media (Staffwise)  Vulnerability and Patch Management Policy |

1. Introduction

The purpose of this Vulnerability and Patch Management Policy is to establish guidelines and procedures for identifying, assessing, prioritizing, and mitigating vulnerabilities within the organization's information systems. This policy aims to ensure the security and integrity of our systems, data, and assets by promptly applying patches and updates to mitigate potential security risks.

1. Scope and key principles  
   This policy applies to all employees, contractors, and third-party vendors who have access to the organization's information systems. It encompasses all hardware, software, networks, and associated components that contribute to the organization's IT infrastructure.

3. Vulnerability Identification:

3.1 The organization shall employ automated vulnerability scanning tools to regularly scan its information systems for known vulnerabilities.

3.2 Employees are encouraged to report any suspected vulnerabilities they encounter to the IT department or designated security personnel promptly.

4. Vulnerability Assessment and Prioritization:

4.1 The IT department shall assess the severity and potential impact of identified vulnerabilities based on industry-standard risk assessment methodologies.

4.2 Prioritization of vulnerabilities shall be based on factors such as severity, exploitability, and potential impact on the organization's assets and operations.

5. Patch Management:

5.1 The IT department shall promptly review and evaluate security patches released by software vendors and third-party providers.

5.2 Critical and high-risk patches shall be applied to affected systems within 30 days of release.

5.3 Regular maintenance windows shall be established to minimize disruption to business operations during patch deployment.

5.4 In exceptional circumstances where immediate patch deployment is necessary to mitigate an imminent security threat, an emergency patching procedure shall be followed.

6. Change Management:

6.1 All patches and updates applied to information systems shall be documented as part of the organization's change management process.

6.2 Changes resulting from patch deployment shall be thoroughly tested to ensure compatibility and minimize the risk of system instability or downtime.

7. Compliance and Reporting:

7.1 Compliance with this policy shall be regularly audited to ensure adherence to established procedures and timelines.

7.2 Security reports detailing vulnerability assessments, patch deployment status, and any outstanding vulnerabilities shall be provided to senior management on a regular basis.

8. Responsibilities

8.1 IT Department: Responsible for conducting vulnerability assessments, prioritizing patches, and deploying updates according to the defined timelines.

8.2 Employees: Required to report suspected vulnerabilities promptly and adhere to security procedures related to patch deployment and system maintenance.

This Policy has been approved and authorised by:

|  |  |
| --- | --- |
| **Name:** | Gemma Lennard |
| **Position:** | Data Protection Officer |
| **Date:** | 08th January 2024 |
| **Due for Review by:** | 08th January 2025 |
| **Signature:** | GL |