Vulnerability & Patch Management Plan

Version Control

Current Version	**1.3**
Released on:	**1-Sep-2025**
Classification	**Internal Use**

Version Number	Date of Release	Nature / Description of Change	Prepared / Changed By	Approved By
1.0	1-Sep-2022	Initial version	Wasim Shaikh	Sujit Karpe
1.1	1-Sep-2023	Second version	Nishant Thool	Sujit Karpe
1.2	1-Sep-2024	Third version	Nishant Thool	Vishal Madan
1.3	1-Sep-2025	Fourth version	Nishant Thool	Vishal Madan

Vulnerability & Patch Management Plan

Purpose and Scope

This Vulnerability Management Policy defines an approach for vulnerability management to reduce system risks and integrate with patch management. From time to time, iMocha may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to iMocha including applicable laws and regulations.

This policy applies to all iMocha assets utilized by personnel acting on behalf of iMocha or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept, and follow all iMocha policies and plans.

Vulnerability and Patch Management Program

iMocha maintains a vulnerability management process that is integrated into the Change Management Process.

iMocha may periodically test the security posture of its applications and systems through third-party testing as well as vulnerability scanning.

iMocha also monitors multiple security alert lists such as the CVE Database and US-CERT to get up to date information on the latest vulnerabilities and threats.

Third-Party Penetration and Vulnerability Tests

Vulnerability and Penetration Testing through External Vendors is conducted on an annual basis. Additional VAPT might be conducted on a need basis in case of significant product changes or introduction of a new product.

Details of our current vendor performing VAPT:

West Advanced Technologies Inc
https://www.wati.com/services/cybersecurity-testing/ - The page also mentions the certifications that the WATI team possesses.

Identifying Vulnerabilities

iMocha reviews third-party penetration test reports and vulnerability scan results to verify vulnerabilities and determine impact.

Scoring Vulnerabilities

Vulnerability & Patch Management Plan

Vulnerabilities are derived from the Common Vulnerabilities and Exposures (CVE) Database and are documented and scored based upon the Common Vulnerability Scoring System (CVSS) standard.

Mitigating Vulnerabilities

If remediation is required, the appropriate team member at iMocha will be notified of the requirements to remediate or mitigate the vulnerability and the time frame of such requirement will depend on the severity and risk of the vulnerability. Such tracking of vulnerabilities must be done through the company's change management tool and in accordance with the Change Management Process.

The information obtained from the vulnerability scanning process will be shared with appropriate personnel throughout the organization on a “need to know” basis to help eliminate similar vulnerabilities in other information systems.

SLAs for Mitigation of Vulnerabilities based on CVSS:

- Critical - 14 days
- High - 30 days
- Medium - 60 days
- Low - 90 days

Patching

All system components, software and production environments shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

System and Non-Company Application Patching
Patching includes updates to all operating systems and third-party applications as provided by the appropriate vendor.

iMocha Application Patching
iMocha applications are patched in accordance with the Change Management Policy. Patches deemed to be of a high or critical nature may be rolled out in a compressed schedule as set forth in such policy.

Patching Exceptions
Patching production systems (e.g., servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigating alternative should be determined through a documented risk analysis.

Exceptions

iMocha business needs, local situations, laws, and regulations may occasionally call for an exception to this policy or any other iMocha policy. If an exception is needed, iMocha management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other iMocha policy or procedure may result in disciplinary action, up to and including termination of employment. iMocha reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. iMocha does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any personnel who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of iMocha as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

iMocha reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Vishal Madan.

This document was last updated on 1/09/2025.