VULNERABILITY MANAGEMENT (TIER 2)

1 Scope

All MBP Pvt Ltd information systems are within the scope of this procedure.

2 Responsibilities

The Sr System Admin is responsible for monitoring vulnerabilities and vendors' releases of patches and fixes and installing operational software updates, patches and fixes on the operational systems.
The Head of Systems Testing is responsible for testing the updated
The Sr System Admin is responsible for the operational (live) environment.
Sr System Admin are responsible for tracking likely vulnerabilities in and patches available for their assets.
The Chief Information Security Officer is responsible for vulnerability risk assessment.

3. Patch Management Policy

3.1 All Workstations, Servers, Software, Cloud Services, System components etc. owned and managed by MBP Pvt Ltd must have a centralized update & Security Patch deployment system (ManageEngine Vulnerability Manager or equivalent) installed to protect the asset from known vulnerabilities.

3.2 Where-ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches must be installed within one month of release from the respective vendor and have to follow the process in accordance with the change control process.

3.3 Regular Patch Management will be carried out on Cloud environments owned and managed by MBP Pvt Ltd regularly, within one month of release, in proper coordination with the Stakeholders of the environment.

3.4 Any exceptions to this process have to be documented & approved by CISO.

4. Procedure [ISO27001 Clause 12.6.1]

4.1 Identified vulnerabilities for organisational assets are prioritized by the level of risk identified during the risk assessment. High-value or high-risk systems are treated ahead of other systems.

4.2 All vulnerabilities that fall into the identified classifications will first be assessed for seriousness and required controls (patching; turning off/removing services affected by the vulnerability; adapting or adding access controls; increased monitoring awareness-raising).

4.3 The required controls will be actioned through the change management procedure (ISMS-C DOC 12.1.2) if they through the incident response procedure (ISMS-C DOC 16.1.5)

4.4 Available patches must be risk assessed, taking into account the balance between risks in installing and not installing, before the final decision as to necessary controls can be made.
4.5 Patches must be tested, as laid down in ISMS-C DOC 12.1.3.
4.6 Vulnerability control decisions are tracked (and can be audited) through either the change management procedure (ISMS-C DOC 12.1.2) or the incident response procedure (ISMS-C DOC 16.1.5).
4.7 The Sr System Admin continuously monitors the vulnerability management, including information about the number of identified vulnerabilities in each organisational asset, what additional controls are in place, what outstanding issues there are, and how the picture has changed since the previous meeting

5. Vulnerability Assessment & Penetration Testing

Vulnerability is something that allows a threat to apply to an asset. In other words, vulnerability is a weak spot that, if not mitigated, allows an attacker to use a specific threat to damage or gain control of a particular asset. For example-vulnerability to threats like fire would be the availability of flammable material such as papers or boxes; or; vulnerability to threats like sabotage or malfunctions could be poor access mechanisms.

MBP Pvt Ltd will run internal network vulnerability scans periodically and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

MBP Pvt Ltd practices more specific and deeper analysis than those offered by Vulnerability Assessment (VA), it performs Penetration Tests (PT)

Parameters:

The general paradigms described above have got very different characteristics according to their field. Three different fields that can be identified are:

- Infrastructure VAs / PTs: they concern all the checks at the wired network, server and client configuration level.
- Application VAs/PTs: they concern all the checks carried out on individual applications.
- Wireless infrastructure PTs: they concern all the checks which are specific to wireless networks.

Moreover, by manually operating on systems and applications, it is also possible to exploit the vulnerabilities that have been found, by completing the attack simulation in order to see the possible consequences in a real situation.

VULNERABILITY MANAGEMENT (TIER 2)

For all vulnerabilities identified during the tests carried out will be generated and documented with sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case. (Screen capture, raw output of security tools, photographs, paper documents, etc.).

As a result of tests performed the below document containing at least the following sections must be generated:

- Introduction
- Executive Summary
- Methodology
- Identified vulnerabilities
- Recommendations for correcting vulnerabilities
- Conclusions
- Evidence

MBP Pvt Ltd and Client Applications deployed in Cloud Environments (including but not limited to VM, platforms-as-service, databases, database-as-service, file systems, files-systems-as-service) would be scanned for vulnerabilities through cloud-softwares or third-party services based on the engagements for all publicly accessible interfaces. The scanned report would be stored in a reproducible way for audit purposes.

Penetration testing of environments and systems must be carried out at the beginning of the system deployment and later, as per the client's needs. Results of the penetration testing would be stored in an accessible location.

All Vulnerabilities found and reported during penetration testing must be remedied and the fixed build be put through the SDLC cycle and deployed in the Production environment as soon as possible but no later than one business week of its reporting.

Document Owner and Approval

The *Chief Information Security Officer* is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to [all/specified] members of staff on the [corporate intranet] and is published.

VULNERABILITY MANAGEMENT (TIER 2)

This procedure was approved by the Chief Information Security Officer (CISO) and is issued on a version-controlled basis under his/her signature.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Zamir Shaikh	24th July 2024