MOHANLAL HEMCHAND PVT L.

VAPT Policy

1. Introduction

Vulnerability Management is a matured outcome of an early day practice of vulnerability assessment. It is imperative for any organization to implement an effective Vulnerability Management to safeguard against attacks and threats in the environment. Vulnerability Management service offers a complete vulnerability management life cycle for finding and remediating security weaknesses before they are exploited and helps with improved visibility to security posture.

1.1. Objective

The overall objective of a Vulnerability Assessment is to scan, investigate, analyze and report on the level of risk associated with any security vulnerabilities discovered on the public, internet-facing devices and to provide MOHANLAL HEMCHAND PVT LTD with appropriate mitigation strategies to address those discovered vulnerabilities.

1.2. Scope

Vulnerability Assessments can be conducted on all asset, product or service within MOHANLAL HEMCHAND PVT LTD.

2. Policy Statements

- MOHANLAL HEMCHAND PVT LTD have a vulnerability management process to ensure the identification and mitigation of any threats to organizational assets.

- **Identify vulnerability and / or patch** – from a range of sources, including but not limited to vendors or other external sources, penetration testing and vulnerabilityscanning shall be performed according to the testing plan, incidents and system monitoring.

- **Risk assess vulnerability** – the identified vulnerability shall undergo risk assessment process to determine the severity of the vulnerability, taking into account:

    - Vulnerability specific variables including ease of vulnerability discovery, ease of exploitation, degree of awareness and likelihood of detection should the vulnerability be successfully exploited.

    - MOHANLAL HEMCHAND PVT LTD’s environment (including network placement) and other information security mitigating controls that may already be in place.

- The outcome of the risk assessment process, including residual risk shall be reported to IT security team.

- **Remediation plan** – assess the risk, if any, of deploying the patch on production systems and identify any flaws, errors or faults arising during deployment. Roll back procedures must be defined. Remediation shall include other actions beyond patching such as decommissioning systems.

- **Execute remediation -** The speed and urgency of execution will be determined by the outcome of the risk assessment.

- **Reporting** - Asset owners shall regularly report on the success of the remediation plan to the security team, including the number of devices that have been remediated and those that remain unremediated.

- **Verification** – Asset owners shall perform and report on verification on the status of patching or alternate remediation plans.

- Remediation shall be undertaken on the following schedule:
  - Very high risk rated vulnerabilities - monthly
  - High risk rated vulnerabilities - monthly
  - Medium risk rated vulnerabilities - quarterly
  - Low risk rated vulnerabilities - quarterly
  - Very Low risk rated vulnerabilities – quarterly
- Post remediation verification process shall be followed.

3. Roles and Responsibilities

Roles	Responsibilities
IT Security Head	▪ Providing and maintaining an enterprise class vulnerability scanner to conduct scans. ▪ Conduct annual compliance reviews of MOHANLAL HEMCHAND PVT LTD ▪ IT SecurityHead is responsible for performing vulnerability risk assessments.
IT Management	▪ Supporting and complying with these policies ▪ Supervising vulnerability assessments and assigning resources ▪ Procuring resources to conduct the vulnerability assessments ensuring that there is no conflict of interest between assessment staff and IT staff ▪ Enforcing this policy.

	▪ Assigning resources for remediation and compliance.
Users	▪ Supporting and complying with this policy ▪ Performing remediation as directed.