BMD SECURITIES LIMITED

PATCH MANAGEMENT PROCEDURE

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	28-04-2025

Version – 1.0

Scope

The objective of this procedure is to proactively monitor the vulnerabilities related to the IT infrastructure used at BMD Securities Limited & patching the known vulnerabilities thereby preventing the IT infrastructure from getting exploited by internal / external threats. This procedure applies to all critical systems, endpoints, applications, and network devices used by the Stock Broker and Depository Participant to maintain cyber hygiene and reduce system vulnerabilities.

Entry Criteria / Inputs

- Software updates from Vendors
- Security patch updates from Vendors / Mailing lists / Website notifications
- Vulnerability assessment reports
- Security Audit reports

Activity Details

Vulnerability Identification

- Regular review of CERT-IN, OEM releases, and threat intel sources for new vulnerabilities.

Patch Schedule

- **Server & Core Infrastructure:** CSP (Cloud Service Provider) to apply latest OS patches within 7 days of release.
- **End-user Systems:** All Windows and Linux endpoints to auto-install patches.
- **Network Devices:** OEM firmware/patch updates must be tracked and applied within 30 days of release.

Roles & Responsibilities

- IT Team to maintain a patch inventory register with patch ID, release date, applied date, and rollback mechanism.
- CISO to approve exception requests with defined timelines and risk assessment.

Audit & Review

- Patch compliance to be reviewed monthly and deviation, if any, to be reported to the Compliance Officer and logged in internal records.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

BMD Securities Limited

BMD SECURITIES LTD.
KOLKATA

Utpal Mallick

Utpal Mallick
CISO
Dated: - 30-04-2025