PP Capital
Your Profit. Our Aim.

PAWAN PARMESHWAR CAPITAL PVT LTD

Regd. Office: 187, Dadiseth Agyari Lane, 4th Floor, Singhania Wadi, Mumbai – 400 002
Head Office: 136-138, ORM Wing B Co-Op Premises Soc. Ltd., Ground Floor, Royal Palm, Goregaon East, Mumbai – 400 065
Tel: 022-22014936 / 4961 3718

Member: NSE Code: 00188 | BSE Code: 0550

Cyber Security and Cyber Resilience Policy

Version 1.0

Policy Title	Cyber Security and Cyber Resilience Policy
Version	1.0
Date of Approval	16th October 2025
Effective Date	20th October 2025
Owner	Information Technology Function with Compliance Department
Approving Authority	Board of Directors of Pawan Parmeshwar Capital Pvt Ltd
Next Review Date	Annually, or earlier upon regulatory change or material cyber incident
Replaces	Not applicable — first formal version under SEBI CSCRF

1. Introduction and Purpose

Pawan Parmeshwar Capital Pvt Ltd ("the Company") is a Stock Broker registered with the Securities and Exchange Board of India ("SEBI") and a Trading Member of the National Stock Exchange of India Ltd (NSE Code 00188) and BSE Limited (BSE Code 0550). The Company is a SEBI-Regulated Entity ("RE") within the meaning of the SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024 (as clarified by SEBI Circular dated April 30, 2025) ("CSCRF").

This Cyber Security and Cyber Resilience Policy ("Policy") sets out the framework within which the Company shall:

- Identify and manage cyber risks to its information systems, client data, and trading operations.
- Protect its IT environment from unauthorised access, malicious activity, and disruption.

- Detect cyber security events on a continuous basis.
- Respond to cyber incidents in a structured and time-bound manner.
- Recover normal operations following a cyber incident.

The Policy is framed for compliance with the CSCRF, the SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025, the Information Technology Act, 2000 and rules thereunder, the CERT-In Directions dated April 28, 2022 (including the 6-hour incident reporting requirement), the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the bye-laws and circulars of the Stock Exchanges and Clearing Corporations, and other applicable Indian law.

2. Categorisation under CSCRF

The CSCRF categorises SEBI Regulated Entities into Market Infrastructure Institutions (MIIs), Qualified REs, Mid-size REs, Small REs and Self-certification REs (and individuals). Categorisation is based on size, scale, and nature of operations of the RE, with specific thresholds set out in the CSCRF.

The Company has, having regard to its size of operations, client base and transaction volumes, assessed itself as a "[Mid-size RE / Small RE — Board to confirm specific categorisation based on latest threshold criteria]" under the CSCRF. The Company shall implement the controls applicable to its category and shall reassess the categorisation annually or upon material change in scale.

Where any provision of the CSCRF applies only to a higher category of REs, the Company shall, as a matter of good practice and progressive maturity, adopt such provisions to the extent practicable having regard to proportionality.

3. Scope and Applicability

This Policy applies to:

- All information systems of the Company including trading systems, back-office systems, client-facing portals (if any), email and messaging systems, financial systems, KYC and CRM systems, surveillance and risk management systems, and the underlying servers, databases, networks, endpoint devices, and cloud / hosted environments.
- All client data, employee data, financial information, trading information, and other information assets in the possession or under the control of the Company.
- All employees, directors, contractors, vendors and third-party service providers having access to the Company's information systems or data.

- All physical and logical access points to the Company's IT environment, including offices, data centres / hosted facilities, remote-working arrangements, and mobile/remote access endpoints.

4. Regulatory Framework

- SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024, as clarified by SEBI Circular dated April 30, 2025 ("CSCRF").
- SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025.
- SEBI (Stock Brokers) Regulations, 1992, including Chapter IVA inserted by SEBI (Stock Brokers) (Amendment) Regulations, 2024 notified on June 27, 2024.
- Information Technology Act, 2000 and rules thereunder, including Section 43A (compensation for failure to protect data) and Section 79 (intermediary obligations).
- CERT-In Directions dated April 28, 2022 (under Section 70B(6) of the IT Act, 2000) requiring reporting of cyber incidents within 6 hours of identification.
- Digital Personal Data Protection Act, 2023 and rules made (or to be made) thereunder.
- National Cyber Security Policy, 2013.
- RBI / CERT-In / NCIIPC advisories and guidelines insofar as applicable to the Company.
- Bye-laws, Rules, Regulations and Circulars of NSE and BSE relating to cyber security and IT systems.

5. Cyber Resilience Goals

The Company adopts the five cyber resilience goals of the CSCRF, which align with the NIST Cybersecurity Framework function categories:

5.1 Identify

Establish and maintain an inventory of information assets, identify cyber risks to those assets, assess vulnerabilities, and define the governance structure for managing cyber risks.

5.2 Protect

Implement appropriate safeguards to limit and contain the impact of a potential cyber security event, including access controls, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

5.3 Detect

Develop and implement appropriate activities to identify the occurrence of a cyber security event in a timely manner, including anomalies and events, continuous security monitoring, and detection processes.

5.4 Respond

Develop and implement appropriate activities to take action regarding a detected cyber security incident, including response planning, communications, analysis, mitigation and improvements.

5.5 Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident, including recovery planning, improvements and communications.

6. Governance

6.1 Board Oversight

The Board of Directors of the Company is the apex authority responsible for cyber security and cyber resilience. The Board:

- Approves this Policy and its periodic revisions.
- Reviews periodic reporting on cyber risk, control posture, incidents and the Company's Cyber Capability Index (CCI) (where applicable to the category).
- Approves the annual cyber security budget.
- Approves the cyber audit programme and reviews findings.
- Takes ultimate responsibility for the Company's cyber security and cyber resilience.

6.2 Designated Officer for Cyber Security

The Company shall designate a senior officer as the "Designated Officer for Cyber Security" ("DO-CS"), with primary responsibility for implementation of this Policy and the CSCRF. The DO-CS shall report to the Compliance Officer and to the Board through periodic reporting. The Board shall record the designation by a separate resolution.

6.3 IT Function

The Information Technology function (whether in-house, outsourced under the Outsourcing Policy v2.0, or a combination) shall be responsible for day-to-day implementation of technical controls under the supervision of the DO-CS and the Compliance Officer.

6.4 Cyber Security Committee (where applicable)

Where required by the CSCRF for the Company's category, or as the Board may determine, a Cyber Security Committee comprising the DO-CS, the Compliance Officer, a representative of senior management, and (where appointed) an external independent cyber security expert shall be constituted to oversee implementation, review incidents, and recommend enhancements.

7. Information Asset Inventory and Risk Assessment

7.1 Asset Inventory

The Company shall maintain an up-to-date inventory of information assets, including:

- Hardware: servers, workstations, laptops, mobile devices, network equipment, dealing terminals, recording infrastructure.
- Software: operating systems, trading applications, back-office systems, antivirus and endpoint protection, communication tools, productivity tools.
- Data: classified into categories such as Public, Internal, Confidential and Restricted (with KYC, financial, trading and UPSI data being Restricted).
- Cloud and outsourced services.
- Network connections, including Exchange connectivity, internet links, VPN endpoints.

The inventory shall be reviewed at least quarterly and on any addition / decommissioning of an asset.

7.2 Risk Assessment

The Company shall conduct cyber risk assessment at least annually and on any material change in the IT environment, threat landscape or regulatory framework. The assessment shall identify:

- Threats: external (cyber-attack, malware, phishing, denial-of-service) and internal (insider misuse, accidental error).
- Vulnerabilities: technical (unpatched software, misconfigurations), procedural (weak processes), human (lack of awareness).
- Impact: confidentiality, integrity, availability of information assets; regulatory, reputational and financial exposure.
- Likelihood: based on threat intelligence, prior incidents, and exposure of the asset.

Risks shall be rated, prioritised and tracked through a risk register. The risk register shall be reviewed by the Board at least annually.

8. Identify — Asset Classification and Data Localisation

Data shall be classified into the following categories:

- Public — information intended for public dissemination (e.g., website content, public disclosures).
- Internal — information for internal Company use that is not sensitive (e.g., internal procedures, general communications).
- Confidential — information that requires protection from unauthorised disclosure (e.g., business plans, employee records, vendor agreements).
- Restricted — information with high sensitivity (e.g., client KYC documents, client trading data, financial information, UPSI, authentication credentials, encryption keys).

Data localisation: To the extent prescribed by the CSCRF and applicable law, data of the Company and its clients shall be stored within India, including primary, replicated and back-up copies. Where data is hosted with a cloud or third-party Service Provider, the Service Provider shall contractually undertake to store data within India in accordance with the Outsourcing Policy v2.0.

9. Protect — Access Controls

9.1 User Identity and Access Management (IAM)

- Every user (employee, contractor, vendor representative) shall have a unique user identifier. Generic and shared accounts are prohibited.
- User access to systems and data shall be granted on the principle of least privilege, with role-based access controls (RBAC) implemented in the trading, back-office, and supporting systems.
- Access requests shall be approved by the relevant business head and IT function, with documentation in an Access Register.
- Access shall be revoked promptly on cessation of employment, change of role, or extended leave.
- Periodic access review (at least half-yearly) shall be conducted by the IT function and reviewed by the DO-CS.

9.2 Authentication

- Strong passwords shall be enforced through password policy (minimum length, complexity, change frequency, prohibition of dictionary words and personal information, no reuse for prescribed cycles).
- Multi-factor authentication (MFA) shall be mandatory for: privileged / administrator accounts; remote access (VPN); access to trading and back-office systems; access to cloud / hosted services; access to financial and KYC systems.

- Authentication credentials shall not be shared, written down in unencrypted form, or stored in unprotected locations.

9.3 Privileged Access

- Privileged accounts (administrator, root, super-user) shall be specifically inventoried and monitored. Their use shall require justification and shall be logged.
- Privileged-session activities shall be subject to additional monitoring controls (where technically feasible).

9.4 Physical Security

- Server rooms, network closets and dealing rooms shall be physically secured with access controls (such as smart-card / biometric access).
- Visitor access shall be controlled, recorded, and escorted.
- Off-site media (back-ups, hard copies of sensitive data) shall be physically secured.

10. Protect — Data Security

- Encryption: Data in transit shall be encrypted (TLS 1.2 or higher) for all external-facing and sensitive internal communication. Data at rest classified as Restricted (such as KYC documents, financial data) shall be encrypted on storage media to the extent technically feasible.
- Removable media (USB drives, external hard disks) usage shall be controlled; default-disabled on endpoints unless explicitly authorised.
- Sensitive data shall not be transmitted through unsecured channels (personal email, public messaging apps, unencrypted file-sharing services).
- Data Loss Prevention (DLP) controls shall be implemented to the extent commensurate with the Company's category under CSCRF.
- Disposal of data: media shall be securely wiped or physically destroyed before disposal; print-outs of sensitive data shall be shredded.

11. Protect — Endpoint, Network and Application Security

11.1 Endpoint Security

- All endpoints (laptops, desktops, dealing terminals, mobile devices used for Company business) shall have current antivirus / endpoint detection-and-response (EDR) protection.
- Operating systems and applications shall be patched in accordance with a documented patch-management cycle, with critical security patches deployed within timelines aligned

to the severity (typically within 7–30 days for critical patches, or earlier as advised by vendor / CERT-In).

- Local administrator privileges on endpoints shall be restricted to authorised personnel.
- Personal devices shall not be used for Company business save in accordance with the Mobile Phone Usage Policy v1.0, the Outsourcing Policy v2.0 and explicit authorisation by the DO-CS.

11.2 Network Security

- Network shall be segmented to isolate critical systems (trading, back-office, KYC) from general-purpose networks (corporate / guest).
- Firewalls shall be deployed at network boundaries; firewall rules shall be reviewed periodically and changes shall be subject to change-management.
- Intrusion detection / prevention systems shall be deployed where commensurate with the Company's category.
- Remote access shall be permitted only through secure channels (VPN with MFA).
- Wireless networks shall be encrypted (WPA2 or higher) with strong pre-shared keys, and guest networks shall be segregated.

11.3 Application Security

- In-house developed applications (if any) shall be subject to secure software development life cycle (SSDLC) practices including code review and security testing.
- Application access shall be controlled through RBAC.
- Application change management shall require testing, approval and rollback procedures.

12. Detect — Logging, Monitoring and SOC

12.1 Logging

- Logs shall be enabled and centrally collected from critical systems including authentication systems, trading systems, back-office systems, firewalls, endpoint protection, network devices, cloud services and email gateway.
- Logs shall be retained for not less than 6 (six) months online and for the prescribed retention period in archival form (as per CSCRF, the Outsourcing Policy v2.0, and the SEBI record-retention framework).
- Logs shall be protected from unauthorised access, modification and deletion.

12.2 Monitoring

- The Company shall establish a security monitoring capability commensurate with its category under CSCRF, which may include subscription to a Market Security Operations Centre (M-SOC) where one is constituted under the CSCRF framework, or arrangements with a managed SOC service provider, or internal monitoring of curated alerts, as appropriate.
- Alerts from monitoring systems shall be triaged, investigated and closed in accordance with the Incident Response procedures.

12.3 Anomaly Detection

- Anomalous activity (unusual login times, geo-location anomalies, large data transfers, repeated failed access attempts, lateral movement patterns, etc.) shall be flagged for investigation.

13. Respond — Cyber Incident Response

13.1 Incident Definition

A "Cyber Incident" includes (but is not limited to):

- Unauthorised access to information systems, accounts or data.
- Data breach (loss, theft, unauthorised disclosure of Restricted or Confidential data).
- Malware, ransomware or other malicious code infection.
- Phishing or social-engineering attack resulting in compromise.
- Denial-of-service or distributed denial-of-service (DoS / DDoS) affecting availability.
- Compromise of cryptographic keys.
- Insider misuse of access.
- Service-provider security incident affecting the Company.
- Any other event that, in the opinion of the DO-CS, materially threatens the confidentiality, integrity or availability of the Company's information systems or data.

13.2 Incident Response Plan

The Company shall maintain a documented Incident Response Plan setting out:

- Identification and triage of incidents.
- Containment measures (isolating affected systems, blocking malicious indicators, revoking compromised credentials).
- Eradication measures (removing malware, patching vulnerabilities, hardening configurations).

- Recovery measures (restoring systems from clean backups, verifying integrity, returning to normal operations).
- Post-incident review and lessons-learnt to feed back into the controls framework.

13.3 Mandatory Incident Reporting

The Company shall, on identification of a Cyber Incident:

- Report to the Indian Computer Emergency Response Team (CERT-In) within 6 (six) hours of identification, in accordance with the CERT-In Directions dated April 28, 2022, where the incident falls within the prescribed categories.
- Report to SEBI in accordance with the CSCRF in the form and timeline prescribed.
- Report to NSE and BSE in accordance with the bye-laws and circulars of the respective Exchanges.
- Report to the Clearing Corporations to the extent that the incident affects clearing and settlement operations.
- Where personal data is affected, comply with the DPDP Act notification obligations to the Data Protection Board of India and to the affected Data Principals as required.
- Inform the Board of Directors within a reasonable time, and the Compliance Officer immediately.

13.4 Communication during Incident

- Incident communication shall be coordinated through the DO-CS in consultation with the Compliance Officer.
- Communications to clients, employees, public and media shall be approved by the Board / Senior Management.
- Speculative communication or internal-source attribution of an incident shall be avoided pending forensic confirmation.

14. Recover — Business Continuity and Disaster Recovery

Recovery from a cyber incident shall be effected in accordance with the Company's Business Continuity Plan (BCP) v1.0 and the Disaster Recovery (DR) arrangements forming part thereof. Key elements include:

- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined for each critical system.
- Regular back-ups, with at least one copy stored off-site / in a different availability zone, and tested restoration.

- Alternate operating arrangements (alternate office, alternate connectivity, alternate dealing terminals).
- BCP / DR testing at least annually, with results documented and reported to the Board.
- Post-incident review and continuous improvement of recovery capabilities.

Cross-reference: Business Continuity Plan v1.0.

15. Vendor and Third-Party Cyber Risk Management

Cyber risks introduced by third parties shall be managed through:

- Due diligence of cyber security posture before engagement (cross-reference: Outsourcing Policy v2.0).
- Contractual provisions for confidentiality, data protection, incident reporting (with timelines no longer than those binding on the Company), audit rights, and right to direct cessation of access in the event of an incident.
- Ongoing monitoring of vendor performance and cyber posture, including review of independent assurance reports (ISO/IEC 27001, SOC 2 Type II, etc.) where applicable.
- Restrictions on sub-contracting and on transfer of data outside India without consent.
- Termination and exit-management provisions ensuring secure return / destruction of data.

16. Cyber Audit and Assurance

The Company shall:

- Engage an independent CERT-In empanelled / equivalent qualified cyber auditor to conduct an annual cyber audit covering the controls under the CSCRF applicable to the Company's category.
- Conduct periodic Vulnerability Assessment and Penetration Testing (VAPT) of externally exposed systems and critical internal systems, at the frequency prescribed under the CSCRF.
- Remediate findings within timelines commensurate with severity, and track remediation through the risk register.
- Submit audit and VAPT reports to SEBI / the Exchanges in accordance with their requirements.
- Report the Cyber Capability Index (CCI) (where applicable to the category) at the prescribed frequency.

17. Training, Awareness and Drills

The Company shall:

- Conduct annual cyber awareness training for all employees, covering phishing recognition, password hygiene, social engineering, secure handling of data, and incident reporting obligations of the employee.
- Conduct phishing simulation exercises at least annually, with retraining of any employees who fall for simulated phishing.
- Conduct incident response tabletop exercises at least annually, involving the DO-CS, the IT function, the Compliance Officer, senior management and (where appropriate) the Board.
- Maintain training records and acknowledgements for the prescribed retention period.

18. Cyber Security Policy Exceptions

Any deviation from this Policy required by operational necessity shall:

- Be documented as a Cyber Security Policy Exception.
- Be approved in writing by the DO-CS and (for material exceptions) by the Compliance Officer.
- Specify compensating controls and a target date for elimination of the exception.
- Be reviewed periodically and reported in the quarterly Board update.

19. Records and Retention

The Company shall maintain records of:

- Asset inventory and risk register.
- Access registers (grants, revocations, periodic-review evidence).
- Logs from systems, networks and applications (online and archival, per Section 12.1).
- Incident registers, including all incidents detected, triaged, resolved or escalated.
- Reports made to CERT-In, SEBI, the Exchanges, the Clearing Corporations and the Data Protection Board (where applicable).
- Cyber audit reports, VAPT reports and remediation evidence.
- Training records, drill reports and tabletop-exercise summaries.
- Cyber Security Policy Exceptions and approvals.

Records shall be retained for not less than 5 (five) years from the date of the event, or such longer period as may be required under CSCRF, IT Act, PMLA, SEBI Master Circular for Stock Brokers, the Registers and Records Manual v1.0, or by reason of any pending proceedings.

20. Roles and Responsibilities

- Board of Directors: Approves this Policy; reviews periodic reporting on cyber risk, incidents, audit findings, CCI (where applicable); approves cyber security budget; designates the DO-CS by separate resolution.
- Designated Officer for Cyber Security (DO-CS): Implements this Policy; conducts annual risk assessment; supervises controls implementation; manages incidents; coordinates cyber audit and VAPT; reports to the Compliance Officer and to the Board.
- Compliance Officer (Mr. Rajkumar Pandey): Oversees regulatory reporting (CERT-In, SEBI, Exchanges, FIU-IND, DPB) in respect of cyber incidents; integrates this Policy with the AML/PMLA, Outsourcing, KYC, and DPDP frameworks; presents cyber matters to the Board.
- Information Technology Function: Implements technical controls; maintains systems; deploys patches; manages logs and monitoring; coordinates with the DO-CS.
- Cyber Security Committee (where constituted): Provides specialist oversight; reviews incidents and audit findings; recommends enhancements.
- Department Heads / Senior Management: Support implementation in their respective functions; ensure their personnel comply; report concerns to the DO-CS.
- All employees: Comply with this Policy; safeguard credentials and devices; recognise and report suspected phishing / social engineering / cyber incidents to the IT helpdesk or DO-CS without delay; cooperate with audit, drills and training.
- Vendors and Service Providers: Comply with their contractual obligations; report incidents within prescribed timelines; cooperate with cyber audits and inspections.

21. Reporting and Review

The Compliance Officer / DO-CS shall present to the Board:

- A quarterly cyber security dashboard covering risk register status, control posture, incidents, exceptions, training metrics, vendor cyber posture and CCI (where applicable).
- An annual cyber audit and VAPT outcome summary with remediation status.
- Material cyber incidents as soon as practicable after detection.
- Communications from SEBI, CERT-In, NSE, BSE, Clearing Corporations or DPB in respect of cyber matters and the response.

This Policy shall be reviewed annually and amended in response to any change in the CSCRF, IT Act, CERT-In Directions, DPDP Act, SEBI / Exchange circulars, or learning from incidents.

Annexure A — Indicative Cyber Security Control Matrix (Summary)

This is a high-level summary of controls. Detailed implementation is documented in IT operational procedures maintained by the DO-CS.

Goal	Indicative Controls
Identify	Asset inventory, data classification, risk register, vendor inventory, regulatory mapping
Protect	IAM with least privilege, MFA, password policy, encryption in transit and at rest for Restricted data, EDR, patching, network segmentation, firewalls, physical security, DLP
Detect	Centralised logging, alert monitoring, anomaly detection, vulnerability scanning, threat-intelligence consumption, M-SOC / managed SOC subscription where applicable
Respond	Incident response plan, response team, 6-hour CERT-In reporting, SEBI/Exchange notification, DPDP notifications where applicable, forensic preservation, communication protocols
Recover	Backup and restore, RTO/RPO definitions, alternate site/connectivity, BCP/DR testing, post-incident review

Annexure B — Cyber Incident Register (Template)

Field	Particulars
Incident Serial Number	
Date and Time of Detection	
Detection Source (SIEM / User Report / Vendor / Other)	
Incident Type	
Severity Classification (Low/Medium/High/Critical)	
Systems / Data Affected	
Confidentiality / Integrity / Availability Impact	
Personal Data Affected (Y/N) — Approximate Count	
Containment Actions and Time	
Eradication / Remediation Actions	
Recovery Actions	
CERT-In Report Filed (Y/N) and Time	
SEBI Report Filed (Y/N) and Time	
Exchange / Clearing Corp Report (Y/N) and Time	
DPB / Data Principal Notification (Y/N) and Time	
Board Notification (Date)	
Root Cause	
Lessons Learnt and Improvements	
Closure Date and Closure Authorised by	

Board Approval

This Cyber Security and Cyber Resilience Policy (1.0) has been reviewed and approved by the Board of Directors of Pawan Parmeshwar Capital Pvt Ltd at its meeting held on 16th October 2025.

The Board has also recorded, on the same date, the following:

- The Board approves this Cyber Security and Cyber Resilience Policy as the framework for compliance with the SEBI CSCRF dated August 20, 2024 (as clarified on April 30, 2025), the SEBI Master Circular for Stock Brokers dated June 17, 2025, the CERT-In Directions dated April 28, 2022, the IT Act, 2000, and the DPDP Act, 2023.
- The Board confirms that the Company's categorisation under CSCRF shall be assessed and ratified by separate Board resolution within 30 days of the Effective Date, having regard to the latest thresholds in the CSCRF.
- The Board shall, by a separate resolution, designate the Designated Officer for Cyber Security (DO-CS) referred to in Section 6.2 of this Policy.
- The Board confirms Mr. Rajkumar Pandey as the Compliance Officer responsible for regulatory reporting in respect of cyber matters (CERT-In, SEBI, NSE, BSE, Clearing Corporations, DPB) and for integration of this Policy with the broader compliance framework.
- The Board ratifies the principle of data localisation within India for the Company's and its clients' data and directs management to ensure that all Service Provider contracts reflect this principle in accordance with the Outsourcing Policy v2.0.
- The Board ratifies the requirement of annual cyber audit (CERT-In empanelled auditor), periodic VAPT, annual BCP / DR testing, annual cyber-awareness training, and annual phishing simulation and tabletop exercises.
- Cross-references to related policies (Business Continuity Plan v1.0, IT and Data Privacy (DPDP) Policy v1.0, Outsourcing Policy v2.0, KYC Policy v2.0, AML/PMLA Policy v2.0, Mobile Phone Usage Policy v1.0, Order Acceptance Policy v2.0, Registers and Records Manual v1.0) are noted.

For PAWAN PARMESHWAR CAPITAL PVT. LTD.

Director / Authorised Signatory

Director / Authorised Signatory

Name: Pawankumar Choudhary

Designation: Designated Director

Place: Mumbai | Date: 16th October 2025