



Vardhaman Capital Private Limited

INFORMATION SECURITY POLICY

Regulatory reference: SEBI CSCRF (Circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113) and applicable clarifications / successor circulars / Cert-In Directions / DPDP Rules 2025

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	17/04/2026
Policy Approved by	Board of Directors
Policy approved on	17/04/2026

Version - 3.0

Purpose

The purpose of this Policy is to safeguard information belonging to the Company and its stakeholders, including third parties, clients, customers and the public, by protecting confidentiality, integrity, availability, privacy and cyber resilience within a secure environment.

This Policy sets the minimum information-security principles for Company staff, directors, contractors, consultants, vendors and other authorised users. It governs the creation, holding, use, sharing, storage, monitoring, retention and disposal of information and supporting technology.

It is the goal of the Company that:

- Information and systems are protected against unauthorised access, misuse, loss, alteration, disclosure or destruction.
- Confidentiality, integrity, availability, authenticity and privacy are maintained in accordance with risk and business need.
- Cybersecurity risks are identified, assessed, treated, accepted or escalated through a documented risk-management process.
- Critical services and information systems remain resilient, recoverable and available for service delivery.
- Business continuity, disaster recovery, backup and incident-response arrangements are maintained and tested.
- Regulatory, contractual, legal and data-protection requirements are identified and complied with.
- Physical, logical, environmental, communication, cloud and endpoint security controls are implemented proportionately.
- Breaches of this Policy may result in disciplinary action, contractual remedies or criminal / regulatory referral, as appropriate.
- Information is retained only for an approved purpose and period and disposed of securely when no longer required.
- Information-security incidents are promptly reported, investigated, contained, recovered from and learned from through the approved incident-response process.

This Policy applies to:

- Information in any form, including electronic records, paper records, communications, images, audio, video, backups and metadata, whether created, received, processed or stored by the Company.
- Company-owned, managed, hosted, cloud-based or third-party technology, networks, applications, endpoints, databases, websites, collaboration services and remotely accessed systems.
- Hardware, software, data, accounts, cryptographic keys, removable media and other information assets owned, leased, used or administered by the Company.
- Information processing undertaken by staff, directors, contractors, consultants, service providers and any other party acting for or on behalf of the Company.
- Electronic recording devices, CCTV systems and any personally owned device approved for business use under the Remote Working and BYOD requirements.

The Policy

The Company requires all users to exercise due care in the operation and use of information systems, to follow approved procedures and to promptly report suspected weaknesses, misuse, loss or security incidents.

Authorised users of information systems

- Except for information published for public consumption, all users of Company information systems must be formally authorised. Each user must have a unique identity; access must be granted on a need-to-know and least-privilege basis; and multi-factor authentication (MFA) must be used where required by risk, including for privileged, remote, cloud and externally accessible access. Credentials, tokens and authentication factors must never be shared.
- Authorised users must protect Company information in their possession and follow the applicable classification, handling and approved-transfer requirements. Confidential, personal or private information must not be copied, transported, shared or uploaded to a third-party service unless authorised and appropriately protected.
 - the information owner's authorisation, the intended recipient and the minimum information necessary for the purpose
 - the classification, privacy, legal, regulatory and contractual risks of loss, disclosure, alteration or use by an unauthorised person
 - the approved secure method for transfer, storage and use at the destination, including encryption where required

Acceptable use of information systems

- Use of the Company's information systems by authorised users must be lawful, ethical, secure and for legitimate business purposes. Users must not bypass security controls, install unauthorised software, use Company resources for prohibited activity or expose Company data to unapproved services. Subsidiary policies may prescribe additional acceptable-use requirements.

Information System Owners

- Designated Officer / Chief Technology Officer / Directors responsible for information systems must ensure that:
 - systems have a named owner, documented business purpose, approved risk classification and controls proportionate to their criticality
 - asset inventories, approved baselines, secure configurations, access controls and physical protections are maintained
 - systems are resilient and available to a level commensurate with their business importance, including defined recovery objectives where applicable
 - data is backed up using approved methods and is demonstrably recoverable through periodic restoration testing
 - data quality, integrity, auditability and authorised change control are maintained throughout the information lifecycle
 - vulnerabilities, security updates, malware protection, endpoint detection and response, and configuration deviations are managed in accordance with risk

- security logs are generated, protected from unauthorised alteration, monitored and retained for the required period; where CERT-In Directions apply, logs must be retained securely in India for at least 180 days on a rolling basis
- third parties entrusted with Company data or systems are assessed, contractually bound and monitored for their information-security responsibilities

Personal Information and Privacy

- The Company may monitor and access Company information systems, communications and records for legitimate business, security, legal, regulatory and investigation purposes, subject to applicable law, notice and approved procedures. Personal information must be processed lawfully, fairly, transparently and securely, with access restricted to authorised persons and only for a defined purpose.
- Individuals who breach this Policy are subject to disciplinary or contractual action at the instigation of the Designated Officer with responsibility for the relevant information system, including referral to law-enforcement or regulatory authorities where appropriate.
- The Company will take reasonable legal, technical and organisational measures to prevent unauthorised use of its information systems and to protect the rights of data principals and other affected persons.

Ownership

- The Designated Officer of ICT Systems is accountable for maintaining this Policy, coordinating the information-security programme, reporting material cybersecurity matters to management / the Board or its committee, and providing guidance on implementation.
- Information-system owners are responsible for implementing this Policy within their areas, maintaining evidence of control operation, addressing identified risks and ensuring that staff and service providers comply with applicable requirements.

Information Security Governance

The Board / designated governing body shall provide oversight of information security and cyber resilience. Management shall establish clear accountability, adequate resources, segregation of duties, measurable objectives and regular reporting on material risks, incidents, control performance and remediation. The Company shall maintain an information-security programme aligned to its business, risk profile and applicable regulatory expectations.

Information Security Risk Management

Information-security risk assessments shall be performed at defined intervals and before material changes, new services, significant suppliers, cloud adoption or processing of sensitive information. Risks shall be recorded with owners, treatment plans, target dates and residual-risk decisions. Risk acceptance requires approval at an authority level proportionate to the risk and shall not override legal or regulatory obligations.

Asset Inventory and Ownership

The Company shall maintain an accurate inventory of information assets, including hardware, software, applications, cloud services, data stores, accounts, integrations, certificates and critical suppliers. Each asset shall have a named

owner, classification, criticality and lifecycle status. Unauthorised, unsupported or end-of-life assets shall be identified, risk treated and removed or isolated in a timely manner.

Data Classification, Handling and Retention

Information shall be classified at least as Public, Internal, Confidential or Restricted, with handling requirements defined for access, storage, transmission, copying, printing, sharing and disposal. Personal data and sensitive business information shall receive protection appropriate to their risk. Records shall be retained only for approved legal, regulatory, contractual and business periods, then securely deleted, anonymised or destroyed with appropriate evidence.

Identity and Access Management

Access shall be provisioned through approved requests, authorised by the relevant information or system owner, and limited to the minimum privileges required. Joiner, mover and leaver processes shall ensure timely creation, review, modification and removal of access. Access to critical systems, data and applications shall be reviewed periodically and immediately when a user's role, employment or business need changes.

Password and Authentication Policy

Passwords shall be unique, kept confidential and protected from disclosure, reuse and storage in insecure locations. Systems shall use strong passphrases, password-deny lists, secure hashing and rate-limiting or equivalent protection against automated attacks. MFA is mandatory for privileged, remote, cloud and externally accessible access, and shall be extended to other high-risk access based on risk assessment. Password changes shall be required on suspected compromise, reset or other defined risk event.

Privileged Access Management

Privileged accounts shall be separately identified, individually assigned, protected by MFA and managed through a controlled privileged-access process. Privileged access shall be time-bound or just-in-time where feasible, approved, logged and reviewed. Shared administrative accounts are prohibited unless technically unavoidable and subject to documented compensating controls, accountability and enhanced monitoring.

Secure Configuration and Change Management

Information systems shall be deployed and maintained using approved secure configuration baselines. Default credentials, unnecessary services, insecure protocols and unsupported components shall be removed, disabled or risk treated. Security-impacting changes shall undergo documented assessment, approval, testing, rollback planning and post-implementation review, with emergency changes reviewed promptly after implementation.

Vulnerability and Patch Management

The Company shall perform vulnerability identification and assessment on a risk-based schedule and after material changes. Security patches and mitigations shall be prioritised by severity, exploitability, asset criticality and exposure, with expedited action for actively exploited or critical vulnerabilities. Where remediation cannot be completed within

the required timeframe, compensating controls, a documented risk decision and a tracked remediation date are required.

Endpoint Protection and EDR

Company-managed endpoints and servers shall use supported operating systems, anti-malware and endpoint detection and response (EDR) or equivalent capabilities appropriate to risk. Controls shall include device encryption where required, host firewalling, application control, secure configuration, patching, removable-media restrictions and central health monitoring. Alerts of suspected compromise shall be investigated and handled under the incident-response process.

Network and Email Security

Networks shall be segmented according to business need and risk, with secure remote access, managed boundary protections and monitoring of suspicious activity. Email shall be protected using anti-phishing, anti-malware, spoofing controls and secure configuration of domains and mail gateways. Users shall verify unusual payment, credential, data-transfer and configuration requests through an independent channel before acting.

Cloud Security

Cloud services may be used only following approved security, privacy, contractual and risk assessment. The Company shall maintain shared-responsibility accountability, strong identity controls, MFA, least privilege, secure configuration, encryption, logging, backup and exit arrangements. Cloud service providers must meet the Company's third-party risk requirements and support applicable data-location, regulatory access, audit and incident-notification obligations.

Encryption and Key Management

Confidential, Restricted and personal information shall be encrypted in transit and at rest where required by classification, risk, law, regulation or contract. The Company shall use approved cryptographic standards and manage keys, certificates, secrets and tokens through controlled generation, storage, access, rotation, backup, revocation and destruction. Private keys and secrets must not be embedded in source code, shared repositories or unapproved documents.

Logging, Monitoring and Threat Detection

Security-relevant activity, including authentication, privileged actions, administrative changes, access to critical data and security events, shall be logged and monitored using appropriate centralised capabilities. Logs shall be time-synchronised, access controlled, protected against alteration and reviewed for suspicious activity. Retention periods shall meet business, legal, regulatory and investigation needs, including any applicable CERT-In log-retention requirement.

Security Incident Response and Reporting

The Company shall maintain and test an incident-response plan covering preparation, detection, triage, containment, eradication, recovery, communications, evidence preservation and lessons learned. Personnel and suppliers shall

promptly report suspected incidents through approved channels. Notifiable cyber incidents shall be reported to CERT-In within six hours of noticing or being brought to notice of the incident, and to SEBI, affected parties or other authorities within applicable requirements and timelines.

Third-Party Risk Management

Before engagement and periodically thereafter, suppliers that access Company information or systems shall be assessed for information-security, privacy, resilience and concentration risks. Contracts shall define security controls, confidentiality, data use, access, sub-processing, audit rights, business continuity, incident notification, return or deletion of data and exit obligations. Material supplier weaknesses shall be tracked to remediation or formally risk accepted.

Secure Systems Development Lifecycle

Where the Company develops, configures or materially changes software, systems shall follow a secure development lifecycle. Requirements shall include security and privacy by design, threat modelling where appropriate, secure coding, code review, dependency and secret management, security testing, segregation of development / test / production environments, controlled release and remediation of identified weaknesses.

Backup, Disaster Recovery and Business Continuity

Business-critical information and systems shall have documented backup, disaster-recovery and business-continuity arrangements, with defined recovery time and recovery point objectives where applicable. Backups shall be protected against unauthorised access and ransomware, with at least one recovery copy isolated or otherwise protected from compromise. Restoration and recovery exercises shall be performed periodically and findings tracked to closure.

Remote Working and BYOD

Remote working shall use approved devices, secure connectivity, MFA and access controls appropriate to the sensitivity of information. Personally owned devices may access Company information only where expressly approved and managed under the BYOD standard, including device security, encryption, screen locking, supported software, remote wipe or containerisation where proportionate. Company data shall not be stored, copied or backed up to unapproved personal services.

Artificial Intelligence and Generative AI Usage

AI and generative-AI tools shall be used only for authorised business purposes and in accordance with risk, privacy, confidentiality, intellectual-property and regulatory requirements. Confidential, Restricted, personal or client information must not be entered into public or unapproved AI services. Users remain accountable for validating AI outputs, protecting data, avoiding discriminatory or unlawful use, and obtaining approval before deploying AI that materially affects customers, operations or regulated activity.

Security Awareness and Training

All personnel shall receive information-security and privacy awareness training at induction and at least annually thereafter, with targeted training for privileged users, developers, finance teams, executives and other high-risk roles.

The programme shall include phishing awareness, secure handling of data, password and MFA hygiene, incident reporting, remote working and AI use. Completion, testing results and corrective actions shall be recorded.

Regulatory Compliance

The Company shall identify, maintain and comply with laws, regulations, regulatory circulars, contractual commitments and industry requirements applicable to its activities. For SEBI-regulated activities, this includes the current SEBI Cybersecurity and Cyber Resilience Framework (CSCRF), relevant category-specific requirements and subsequent clarifications. The Company shall also meet applicable CERT-In Directions and shall prepare for / comply with the Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 in line with their notified commencement and applicability.

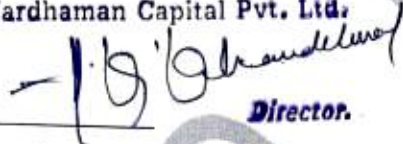
Periodic Review and Policy Exceptions

The Designated Officer shall coordinate periodic review of this Policy, supporting standards and control effectiveness, with updates approved through the Company's governance process. Exceptions are permitted only where they are documented, risk assessed, time-bound, compensated where necessary and approved by the relevant authority. Exceptions shall be monitored, revalidated before expiry and revoked when the business need or risk basis no longer applies.

This Policy shall be reviewed at least annually and sooner following a material change, significant incident, regulatory change, audit finding or risk reassessment. Any exception must be formally documented, risk assessed, time-bound, approved by the appropriate authority and reviewed until it is closed or renewed.

Vardhaman Capital Private Company

For Vardhaman Capital Pvt. Ltd.


Director.

Authorised Signatory

Date: - 17/04/2026