Cyber Security & Data Privacy Policy

V-MARC India Limited

Policy no. VIL-CSDP-001V1 · Version 1.0 · Effective 06-11-2026

Document Details

Item	Details
Policy name	Cyber Security & Data Privacy Policy
Policy no. / Document no.	VIL-CSDP-001V1
Created by	Himanshu Jadon, Head - IT
Execution responsibility	IT Team
Approved by	Board of Directors
Effective date	06-11-2026
Review cycle	Annually, and after any major incident or business change
Document classification	Public (published on the Company's website)

1. Purpose and Scope

V-MARC India Limited ("the Company") is committed to protecting its information systems and the personal data of its employees, customers, vendors, shareholders and other stakeholders. This policy sets out the Company's approach to managing cyber security risks and risks related to data privacy.

The policy applies to all plants, the corporate office, sales offices, depots and warehouses of the Company. It covers every person who uses the Company's information systems, including employees, trainees, contractors, consultants and vendors. It protects information in any form, whether electronic, on paper or spoken. The Company's subsidiaries may adopt this policy with the approval of their own Boards. The policy also extends to the Company's value-chain partners — IT vendors, service providers and contractors who access Company systems or personal data — through their contracts with the Company.

Objectives. The policy aims to protect the confidentiality, integrity and availability of the Company's information:

- Confidentiality: information can be seen only by those who are authorized to see it;
- Integrity: information is accurate and complete, and is not changed without authority;
- Availability: systems and information are available to authorized users when the business needs them.

2. Regulatory framework

The Company follows all applicable laws, rules and directions, including:

- Information Technology Act, 2000 and the rules made under it
- Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025
- Directions by the Indian Computer Emergency Response Team (CERT-In)
- Companies Act, 2013 and the Companies (Accounts) Rules, 2014, for books of account kept in electronic form
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and SEBI (Prohibition of Insider Trading) Regulations, 2015
- Copyright Act amended for software licensing, and the E-Waste (Management) Rules, 2022 for the disposal of IT equipment

3. Governance and responsibilities

Who	Responsibility
Board of Directors	Approves this policy and oversees cyber security and data privacy risks
Audit Committee	Reviews IT and cyber security risks, internal controls and IT audit findings at least once a year
IT Steering Committee (chaired by the Managing Director)	Reviews IT risks, major incidents, projects and policy compliance every quarter
Head of IT	Owns this policy, puts security controls in place and reports to management and the Audit Committee
Company Secretary & Compliance Officer	Assesses incidents for disclosure under SEBI regulations and oversees the Structured Digital Database for price-sensitive information
Head of HR	Handles employee personal data, onboarding and exit of users, and disciplinary action
Department heads and every user	Follow this policy, protect their accounts and devices, and report incidents at once

4. Cyber security commitments

The Company maintains reasonable security practices that are proportionate to its risks, aligned with ISO/IEC 27001 and, for plant operational technology, IEC 62443. In particular:

1. **Information and assets:** Information is classified as public, internal, confidential or restricted and handled accordingly. IT assets have a named owner, are returned when a user leaves, and are disposed of securely, with data erased and equipment recycled under the E-Waste Rules.
2. **Access control:** Each user has a unique ID and only the access their role needs. Multi-factor authentication protects email, remote access and critical systems. Access is removed or changed promptly when a person leaves or changes role, and staff and contractors are bound by confidentiality obligations.
3. **Network and endpoint protection:** Networks are segregated and protected by firewalls. Every device runs managed endpoint protection, and systems are patched regularly.
4. **Remote and mobile working:** Remote working, mobile devices, personal devices and wireless networks may connect to Company systems only under approved and secured arrangements.
5. **Encryption:** Confidential information and personal data are encrypted in transit and, where appropriate, at rest, using approved methods and protected keys.
6. **Shop-floor systems:** Operational technology at the plants is kept separate from the office network, and vendors get controlled, logged access only.
7. **Cloud services and applications:** Cloud services are assessed for security before use. Business applications are developed, tested and changed under controlled procedures, with testing kept separate from live systems.
8. **Physical security:** Server rooms and network areas are access-controlled and protected against unauthorized entry, fire and power failure.
9. **Backup and recovery:** Business data is backed up regularly and restores are tested. Books of account in electronic form are backed up daily on servers located in India, and the accounting software keeps an audit trail.
10. **Logs:** Security logs are kept centrally and protected from tampering. They are retained for at least 180 days within India, as the CERT-In directions require, and for at least one year once the DPDP Rules, 2025 come into force.
11. **Monitoring:** The Company may monitor the use of its systems, networks and email for security and legitimate business reasons, in line with applicable law.
12. **Vendors:** IT vendors are assessed before they are engaged. Their contracts cover confidentiality, security, breach notification and the return or deletion of Company data.
13. **Testing and audit:** Systems are scanned for vulnerabilities and tested by periodic penetration testing, with findings tracked until closed. IT controls are audited at least once a year.
14. **Business continuity:** The Company keeps a disaster recovery plan and tests it at least once a year, so that critical operations can continue during an outage.

5. Data privacy commitments

The Company processes personal data of employees, customers, vendors and shareholders lawfully and fairly. It:

- collects personal data only for a clear and lawful purpose, with notice and consent where the law requires it;
- collects only the minimum data needed and keeps it accurate;
- restricts access to those who need it, and protects personal data with safeguards such as encryption, access control and logging;
- keeps personal data only as long as the purpose or the law requires, and then erases it securely;
- does not share personal data with third parties except for business needs under a contract, or where the law requires it;

- transfers personal data outside India only as permitted under the Digital Personal Data Protection Act, 2023;
- respects the rights of individuals to obtain information about their personal data, to have it corrected or erased, to withdraw consent, to nominate another person to exercise their rights in the event of death or incapacity, and to raise a grievance;
- gives a plain-language privacy notice when it collects personal data, saying what is collected and why;
- processes the personal data of children only with the verifiable consent of a parent or lawful guardian, as the law requires;
- treats unpublished price-sensitive information as restricted, and keeps the Structured Digital Database under the SEBI insider trading regulations with time-stamping and an audit trail.

Personal data of shareholders kept by the Company's Registrar and Share Transfer Agent is handled under the agreement with the Registrar and SEBI requirements.

Website. Personal data collected through the Company's website, for example through enquiry forms, is used only for the purpose for which it was given.

6. Incident management and disclosure

Every suspected cyber security incident or personal data breach must be reported to the IT team at once. IT contains and investigates it, preserves evidence, restores normal working, finds the root cause and records the lessons learned. Corrective and preventive actions are tracked until closed and reported to the Audit Committee and Board. The Company maintains a register of cyber security incidents and personal data breaches, recording the nature of each incident, whether personal data of customers was involved, its impact and the corrective action taken.

Report to	When
CERT-In, for reportable cyber incidents	Within 6 hours of noticing the incident
Data Protection Board of India and the affected individuals, for personal data breaches	Without delay, with a detailed report to the Data Protection Board within 72 hours, under the DPDP Rules, 2025
Company Secretary & Compliance Officer	At once, for any incident that may be material
Stock exchange (where the Company's shares are listed)	Within the time set by Regulation 30 of the SEBI LODR Regulations, if the incident is found material under the Company's Materiality Policy
Audit Committee and Board	In the next periodic report on cyber security, or earlier for a major incident

7. Awareness, compliance and review

Training: New joiners complete IT and information security induction in their first week. All users take refresher training and phishing-awareness exercises at least once a year.

Compliance: A breach of this policy may lead to disciplinary action, up to termination of employment or contract. Suspected violations of law may be referred to the authorities.

Reporting violations: Anyone who becomes aware of a violation of this policy should report it to the Head of IT or through the Company's vigil mechanism (whistle-blower policy). The Company does not tolerate retaliation against anyone who reports in good faith.

Review: The Head of IT reviews this policy at least once a year, and earlier after a major incident or a change in law. Changes are approved by the Board Minor or administrative changes to the internal IT Policy and its procedures may be approved by the Managing Director and placed before the Board for noting.

8. Commitments and targets

The Company has set the following annual targets. Performance against them is reviewed by the Audit Committee and reported in the Company's Business Responsibility and Sustainability Report (BRSR):

- Zero material cyber security incidents and zero personal data breaches.
- 100% of users with access to Company systems complete information security awareness training every year.
- An IT and cyber security audit every year, with high-risk findings closed within agreed timelines.
- At least one disaster recovery test and one cyber incident exercise every year.
- All privacy and cyber security grievances acknowledged and resolved within the timelines prescribed by law.

9. Contact

Grievances are acknowledged promptly and resolved within the timelines prescribed under the Digital Personal Data Protection Rules, 2025, and a record of all grievances is maintained. Queries or grievances about cyber security or personal data can be sent to:

Contact	Details
Personal data and privacy queries	Abhay Goel (AGM-HR), hr@v-marc.in
Cyber security and IT	Himanshu Jadon (Head IT), head.it@v-marc.in
Investors and shareholders	Anuj Ahluwalia (CS & Compliance Officer), cs@v-marc.in

VIKAS GARG Digitally signed by VIKAS GARG Date: 2026.11.06 16:15:41 +05'30'