VIRGO®
GROUP

INFORMATION SECURITY & DATA PRIVACY POLICY

[POLICY START DATE - 12th March, 2026]
[DATE LAST UPDATED - 15th July, 2026]

Virgo Group
Information Security & Data Privacy Policy

Approved By: Board of Directors, Virgo Group

1. Purpose & Commitment

Virgo Group is committed to protecting the confidentiality, integrity, and availability of all business, financial, technical, and personal information entrusted to it. This policy establishes mandatory standards for data security, privacy, and compliance across all group companies, in alignment with global best practices, applicable Indian regulatory requirements (including the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023), and ISO/IEC 27001 principles. This policy is mandatory and shall be binding on all employees and associated persons.

2. Scope

This policy applies to all group entities (Virgo Laminates Ltd., Virgo Aluminum Ltd., Virgo ACP Industries Pvt. Ltd., Virgo Plywoods Ltd., Virgo MDF Pvt. Ltd., Virgo Graphics Pvt. Ltd., Higgs Healthcare Ltd., and affiliates), as well as to all employees, directors, contractors, vendors, consultants, third-party partners, and associated persons. "Associated Persons" shall include interns, trainees, temporary staff, agency personnel, secondees, advisors, representatives, and any other individual granted access to Company information, systems, premises, or assets. It further applies to all information assets, including digital records, physical documents, verbal communications, and intellectual property. This Policy applies irrespective of the location from which Company work is performed, including office premises, manufacturing facilities, remote work locations, client sites, and while travelling.

This policy covers all forms of data, including:

a. Digital data
b. Physical records
c. Verbal information
d. Strategic, financial, and technical information

3. Policy Principles

(i) Confidentiality – Information shall only be accessible to authorized personnel.
(ii) Integrity – Information shall be accurate, complete, and safeguarded.
(iii)Availability – Information shall be accessible to authorized users when required.

(iv) Accountability – Every employee is individually responsible for protecting company data.

(v) Compliance – All processing of data shall adhere to applicable laws and contractual obligations.

(vi) Personal data shall be collected, processed, stored, shared, and retained only for legitimate business, employment, legal, compliance, and operational purposes and in accordance with applicable data protection laws.

(vii) Least Privilege – Access to Company information shall be granted strictly on the basis of business necessity and least privilege.

(viii) Privacy by Design – Systems and business processes involving personal data shall incorporate privacy and security controls by design and by default.

4. Data Handling & Access Control

4.1. Any unauthorized attempt to access, download, copy, extract, modify, transmit, or disclose Company information beyond an individual's authorized access rights shall constitute a violation of this Policy and may result in disciplinary and legal action.

4.2. Access to systems and confidential data shall be role-based and granted on a need-to-know basis. Strong authentication (password + biometric) is mandatory for all company devices and systems. Personal devices must not be used for company data without written approval. Information shall be classified as Confidential, Restricted, Internal, or Public and handled accordingly. All removable media, printouts, and files shall be disposed of securely.

4.3. **Google Sheets Usage Policy**

4.3.1. Google Sheets may only be used for company data with explicit prior approval from department heads or DME, aligning with existing cloud storage restrictions.

4.3.2. Key mandates include: Approval and Classification: All Sheets containing company data (e.g., sales, customer, financial info) require written approval before creation. Classify as per policy (Confidential/Restricted) and store in company-approved Google Workspace drives only. Apply principle of least privilege—share only with specific authorized users/groups via Google Workspace domains. Disable "Anyone with the link" and set view-only/edit restrictions as needed. Appropriate access controls, sharing restrictions, and security settings shall be implemented to prevent unauthorized access, modification, or disclosure. No sharing with external/non-approved users, no IMPORTRANGE from unauthorized sheets, no screenshots or exports without approval. Regularly review version history and activity logs for unauthorized changes. Enable 2-Step Verification (2FA) on all accounts; avoid public Wi-Fi access. Violations treated as data leakage under zero-tolerance policy.

4.4. Passwords must contain a minimum of 12 characters and include uppercase letters, lowercase letters, numbers, and special characters. Passwords shall not be shared, reused across systems, or written in unsecured locations. Multi-Factor Authentication (MFA) shall be enabled wherever available.

5. Data Management

All Company data shall be stored only on Company-approved systems and locations. Employees shall ensure that data is accurate, complete, backed up where required, retained in accordance with Company retention requirements, and securely disposed of when no longer required.

6. Confidential Information

6.1. "Confidential Information" means all non-public information relating to the Company, its affiliates, customers, suppliers, employees, operations, finances, products, technology, strategies, business plans, pricing, trade secrets, intellectual property, and any information designated as Confidential, Restricted, Internal, Proprietary, or Sensitive.

6.2. Employees shall not disclose, copy, transmit, retain, remove, use, or permit access to Confidential Information except as required for authorized Company business. All Confidential Information shall remain the exclusive property of the Company, and confidentiality obligations shall continue during and after employment. Trade Secrets and proprietary information shall remain confidential indefinitely and shall survive termination of employment.

6.3. Employee records, salary details, compensation information, attendance records, performance evaluations, disciplinary records, personal information, medical information, identification documents, and HR records are strictly confidential and shall not be disclosed without written authorization from HR or Management.

7. Authorized Software Usage

Employees shall install and use only Company-approved and properly licensed software on Company devices and systems. Installation, downloading, copying, or use of any pirated, cracked, unlicensed, or unauthorized software is strictly prohibited. Any requirement for new software shall require prior approval from the Company. Violation of this provision may result in disciplinary and legal action.

8. Device & Network Security

8.1. Only company-approved laptops, mobile devices, software, and VPNs may be used for all official work. Access to company systems over public or unsecured Wi-Fi networks is strictly prohibited. Remote access shall be permitted only through a secure VPN with multi-factor authentication (MFA).

8.1.1. Only company-approved devices are permitted

8.1.2. Use of personal devices is prohibited unless explicitly approved

8.1.3. Access via public or unsecured Wi-Fi is not allowed

8.2. Use of removable media, including USB drives, external storage devices, and similar media, is prohibited unless specifically authorized by the Company for legitimate business purposes. Employees are also prohibited from installing and using any unauthorized software.

8.3. Employees shall not upload, input, copy, paste, or otherwise disclose any Company confidential information, customer information, employee information, financial information, contracts, source code, designs, pricing information, business strategies, or internal documents into public Artificial Intelligence platforms (including ChatGPT, Gemini, Claude, Copilot, DeepSeek, Grok, or similar services) unless expressly approved in writing by the Company. AI-generated outputs shall not be relied upon for legal, financial, technical, or business decisions without appropriate review and approval.

8.4. Passwords must contain a minimum of 12 characters and include uppercase letters, lowercase letters, numbers, and special characters. Passwords shall not be shared, reused across systems, or written in unsecured locations. Multi-Factor Authentication (MFA) shall be enabled wherever available.

9. Communication & Collaboration

9.1. All business communication shall be through official email domains, and registered numbers. Use of WhatsApp or similar apps is allowed only via registered numbers. Forwarding sensitive documents/screenshots to personal accounts is prohibited.

9.2. Employees shall obtain prior written approval from their Reporting Manager or the authorized approving authority before sending any email containing legal commitments, quotations, pricing, discounts, commercial offers, contractual terms, settlement proposals, or any communication capable of creating financial or legal obligations on behalf of the Company.

9.3. **Zero Tolerance on Data Leakage**

9.3.1. Unauthorized sharing of company data is strictly prohibited under all circumstances.

9.3.2. This includes sharing with:

(i) Competitors, ex-employees, friends, or family
(ii) Vendors or third parties without approval

9.4. **Covered data includes:** Sales, purchase, pricing, customer data, designs, and financial or strategic information.

9.5. **Mobile & WhatsApp Security:** Any communication conducted for Company business through approved communication channels shall constitute Company business records and remain subject to this Policy.

9.6. **Strictly prohibited:**

9.6.1. Transferring chats to personal accounts

9.6.2. Taking backups on personal cloud storage (Google Drive, iCloud, etc.)

9.7. On exit: Mandatory logout and handover of communication data. Violations shall be treated as data breach and may lead to legal action.

9.8. **Email Signature Format:** All employees must use a uniform email signature across official domains to ensure branding consistency, compliance, and security—no personal variations allowed. HR will enforce via Gmail.

9.9. **Cloud & Storage Restrictions:** Use of personal cloud platforms (Google Drive, Dropbox, iCloud, etc.) is not permitted.
All data must be stored only on company-approved systems.

9.10. **Screenshot & Recording Policy:** Screenshots, screen recording, or data copying are strictly prohibited without prior approval.

9.11. **Employee Exit & Separation**

9.11.1. Upon demand by the Company or upon cessation of employment, employees shall immediately return all Company property and Confidential Information and permanently delete any Company information stored on personal devices or media, and shall provide written certification of compliance if required by the Company. Any violation shall be treated as a serious breach and may result in legal action, including proceedings under applicable laws. The Company may require reasonable evidence or certification confirming completion of data deletion obligations.

9.11.2. Employees shall not retain any copy, extract, summary, screenshot, photograph, backup, reproduction, or derivative record of Confidential Information after cessation of employment unless expressly authorized in writing by the Company.

10. Incident Management

10.1. All actual or suspected data breaches, unauthorized disclosures, malware incidents, compromised credentials, unauthorized access, lost or stolen devices, or any incident that may adversely affect the confidentiality, integrity, or availability of Company information, systems, or assets must be reported immediately upon discovery to the Employee's Reporting Manager, HR Department, or any other designated authority of the Company. The Company shall investigate, document, and take appropriate action in relation to all reported incidents. Failure to promptly report a known or suspected security incident may constitute a serious violation of this Policy and may result in disciplinary and/or legal action.

10.2. Employees shall remain vigilant against phishing emails, suspicious emails, fraudulent links, malware, social engineering attacks, fake invoices, impersonation attempts, and other cybersecurity threats. Employees shall not open, respond to, click on, download from, or forward any suspicious email, attachment, link, or communication and shall immediately report the same to the Company's designated authority.

10.3. Employees shall fully cooperate with any audit, inquiry, investigation, forensic review, compliance assessment, or incident response conducted by the Company

and shall preserve all relevant records, communications, devices, credentials, and information as may reasonably be required for such purpose.

11. Digital Monitoring & Surveillance

11.1. The Company reserves the right to monitor and review employee activities on its systems to ensure security, compliance, and operational integrity. This includes monitoring of emails, system usage, device activity, file transfers, WhatsApp Web, and ERP systems. Periodic audits may be conducted to assess adherence to this policy.

11.2. Any violation may result in disciplinary action, up to and including termination of employment and legal proceedings. Employees acknowledge and consent to monitoring, review, audit, recording, and investigation of activities conducted on Company-owned systems, devices, networks, applications, email systems, ERP platforms, and business communication channels for legitimate business, security, compliance, and legal purposes, in accordance with applicable law.

11.3. Electronic records, system logs, access logs, audit trails, email records, metadata, CCTV records, and other digital evidence maintained by the Company may be relied upon for investigation, disciplinary action, audit, compliance review, arbitration, or legal proceedings, subject to applicable law.

12. Hardware Security

12.1. Employees are responsible for safeguarding all Company-issued laptops, desktops, mobile phones, storage devices, ID cards, access cards, SIM cards, peripherals, and other Company assets against theft, loss, damage, misuse, or unauthorized access. Any loss, theft, damage, or suspected compromise shall be reported to the Company immediately upon discovery. Upon suspension, transfer, demand by the Company, or cessation of employment for any reason, employees shall promptly return all Company-issued hardware, devices, accessories, identification cards, storage media, and other assets in good condition (subject to normal wear and tear) and shall not retain any Company property or copies of Company data.

13. Non-Compete & Non-Solicitation

13.1. For a period of twenty-four (24) months following cessation of employment, the Employee shall not directly or indirectly solicit, induce, divert, or attempt to solicit any customer, distributor, supplier, vendor, business partner, or employee with whom the Employee had material dealings during the course of employment.

13.2. The Employee shall remain bound by confidentiality obligations relating to all Confidential Information, Trade Secrets, customer information, pricing information, strategic information, technical information, and proprietary business information acquired during employment.

14. Intellectual Property

14.1. All reports, analyses, databases, software, designs, processes, documents, presentations, customer information, pricing information, strategic plans, inventions, developments, and other work products created, developed, or contributed by an Employee during the course of employment shall be the sole and exclusive property of the Company.

14.2. Employees shall not create, register, purchase, reserve, or use any domain name, company name, trade name, trademark, email address, social media account, website, mobile application, Google Business profile, or other digital asset that is identical or confusingly similar to the Company's name, brands, subsidiaries, products, or trademarks for personal purposes under any circumstances. Creation or use for legitimate Company business shall require prior written approval from the Managing Director or other authorized authority.

15. Financial Liability & Damages

15.1. Any employee who intentionally, fraudulently, wilfully, or through gross negligence causes loss to the Company through violation of this Policy shall be liable for all proven losses, damages, investigation costs, legal expenses, remediation costs, and liabilities incurred by the Company, to the extent permitted by law.

15.2. The Company reserves the right to seek recovery of such losses and pursue all legal remedies available under applicable law

16. Emergency Action Rights

The Company may immediately suspend system access, preserve evidence, secure Company assets, and initiate investigation measures where necessary to protect Company information, systems, business interests, or legal rights.

17. Legal & Regulatory Compliance

17.1. This policy aligns with the Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, and confidentiality obligations. Breach may result in civil, criminal, and financial liabilities.

17.2. **Violations may lead to:**

17.2.1. Disciplinary action, including termination of employment

17.2.2. Legal proceedings under applicable laws

17.2.3. Civil and criminal liability

18. Injunctive Relief

The Employee acknowledges that unauthorized disclosure, misuse, retention, or transfer of Confidential Information may cause irreparable harm to the Company. The Company shall be entitled to seek immediate injunctive relief, interim relief, specific performance, and other remedies available under law without prejudice to any other rights or claims.

19. Vendor & Third-Party Access

19.1. All vendors, contractors, consultants, and service providers who are granted access to Virgo Group information or systems must:

19.1.1. Sign a Non-Disclosure Agreement (NDA) prior to accessing any data.

19.1.2. Comply fully with this Information Security & Data Privacy Policy, as well as applicable laws and contractual obligations.

19.1.3. Use Virgo-approved secure communication channels and systems for all interactions involving company data.

19.1.4. The Company reserves the right, subject to applicable contractual and legal requirements, to verify, review, audit, inspect, or otherwise assess compliance with information security, confidentiality, data protection, and access control obligations by any vendor, contractor, consultant, or third-party service provider granted access to Company information or systems.

20. Responsibilities

20.1. Effective implementation of this Policy requires participation and accountability at all levels of the organization. The following responsibilities apply:

20.1.1. Management: Ensure adequate resources, governance, oversight, and support for implementation and enforcement of this Policy.

20.1.2. HR: Facilitate policy communication, employee awareness, training, acknowledgment, and exit compliance requirements.

20.1.3. Employees: Read, understand, and comply with this Policy, protect Company information and assets, and promptly report any actual or suspected security incidents, data breaches, or policy violations.

21. Review & Updates

21.1.1. This Policy may be amended, modified, replaced, supplemented, or updated by the Company from time to time at its sole discretion. The latest version of this Policy shall be uploaded on the Company's official website and may also be circulated through official Company communication channels, including WhatsApp, or other authorized means. Such revised Policy shall become effective from the date specified therein.

21.1.2. It shall be the responsibility of every employee and associated person to periodically review the latest version of this Policy, remain informed of all amendments, and ensure continuous compliance with the Policy as amended from time to time. Failure to read or acknowledge any amendment shall not exempt any employee or associated person from compliance with the revised Policy.

21.1.3. The Policy shall be deemed to have been duly communicated upon its publication on the Company's official website or circulation through any authorized communication channel. Every employee and associated person is responsible for

regularly reviewing the Company's official website and other authorized communication channels to remain updated with the latest version of the Policy and any amendments thereto.

22. Policy Communication & Acceptance

22.1. This Policy is applicable to all employees and associated persons of the Company. The Company may communicate this Policy and any amendments thereto through its official website, email, WhatsApp, or any other authorized communication channel. The latest version of this Policy shall be available on the Company's official website.

22.2. This Policy shall become effective and binding immediately upon its publication on the Company's official website or communication through any authorized communication channel. No separate acknowledgment, undertaking, or signature shall be required for this Policy to become valid and enforceable. Continued employment, engagement, or continued access to the Company's systems, information, premises, facilities, or other resources after such communication shall constitute deemed acceptance of and agreement to comply with this Policy, as amended from time to time.

22.3. Employees and associated persons shall periodically review the latest version of this Policy available on the Company's official website and shall remain responsible for keeping themselves informed of all amendments and revisions. Failure to review this Policy or any amendment shall not affect its applicability or enforceability.

22.4. Compliance with this Policy, as amended from time to time, is a mandatory condition of employment, engagement, and continued access to the Company's systems, information, premises, facilities, and other resources.

23. Final Declaration

Non-compliance may result in disciplinary action, including termination of employment where appropriate, and may result in civil, criminal, contractual, or regulatory proceedings where warranted by the nature and severity of the violation.

Last Amended On: 15th July, 2026