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 Aluminium 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. It further applies to all information assets, including digital records, physical documents, verbal communications, and intellectual property.

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

1. Confidentiality – Information shall only be accessible to authorized personnel.
2. Integrity – Information shall be accurate, complete, and safeguarded.
3. Availability – Information shall be accessible to authorized users when required.
4. Accountability – Every employee is individually responsible for protecting company data.
5. Compliance – All processing of data shall adhere to applicable laws and contractual obligations.

4. Data Handling & Access Control

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.

Google Sheets Usage Policy

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

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. Use "Protect sheets and ranges" (Data > Protect sheets and ranges) to lock sensitive cells/ranges. 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.

5. Device & Network Security

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).

a. Only company-approved devices are permitted
b. Use of personal devices is prohibited unless explicitly approved
c. Access via public or unsecured Wi-Fi is not allowed

The following are strictly prohibited:

a. Use of USB drives or pen drives
b. Use of external hard disks
c. Installation or use of unauthorized software

6. Communication & Collaboration

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.

Data Leakage – Zero Tolerance

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

This includes sharing with:

a. Competitors, ex-employees, friends, or family
b. Vendors or third parties without approval

Covered data includes:

Sales, purchase, pricing, customer data, designs, and financial or strategic information.

Mobile & WhatsApp Security

Any number used for company work shall be treated as a Company Communication Asset.

Strictly prohibited:

a. Transferring chats to personal accounts
b. Taking backups on personal cloud storage (Google Drive, iCloud, etc.)

On exit:

- Mandatory logout and handover of communication data

Violations shall be treated as data breach and may lead to legal action.

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.

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.

Screenshot & Recording Policy

Screenshots, screen recording, or data copying are strictly prohibited without prior approval.

Employee Exit & Separation

Employees leaving the organization must return all company assets, delete all company data from personal devices, submit a data deletion declaration, and refrain from any post-exit use or disclosure of company information. Any violation shall be treated as a serious breach and may result in legal action, including proceedings under applicable laws.

7. Incident Management

All suspected breaches, phishing attempts, lost devices, or unauthorized access must be reported immediately to HR. There team will investigate and document incidents.

The following must be reported immediately:

a. Data breaches
b. Suspicious emails or phishing attempts
c. Lost or stolen devices

Any delay in reporting shall be treated as a **serious violation of company policy**

8. Digital Monitoring & Surveillance

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.

Any violation may result in disciplinary action, up to and including termination of employment and legal proceedings. Employee consent to such monitoring shall be deemed granted by virtue of use of company systems and resources.

9. Non-Compete & Non-Solicitation

For 12–24 months after exit:

Employee cannot:

a. Join competitor in same role
b. Start competing business
c. Contact company clients

10. Financial Liability & Damages

Employee will be liable for:

a. Business loss
b. Future impact
c. Reputation damage

Company may:

a. Deduct salary
b. Recover damages legally

11. Emergency Action Rights

Company may:

a. Block access instantly
b. Seize devices
c. Suspend employee

12. Legal & Regulatory Compliance

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.

Violations may lead to:

a. Disciplinary action, including termination of employment
b. Legal proceedings under applicable laws
c. Civil and criminal liability

13. Responsibilities

Vendor & Third-Party Access

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

1. Sign a Non-Disclosure Agreement (NDA) prior to accessing any data.
2. Comply fully with this Information Security & Data Privacy Policy, as well as applicable laws and contractual obligations.

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

Management: Ensure resources, governance, and oversight.
HR: Enforce training and exit compliance.
Employees: Adhere to this policy and report breaches.

14. Review & Updates

This policy will be reviewed annually or upon significant regulatory/technological changes. Updated versions will be circulated to all employees.

15. Acknowledgment

Every employee and third-party partner must sign an acknowledgment confirming understanding and acceptance of this policy.

Please refer Annexure A and sign it.

16. Policy Acceptance (Very Important)

This policy is circulated via:

a. Email
b. WhatsApp
c. Official communication

If no objection is received within 7 days:

a. Policy is deemed accepted
b. Legally binding on employee

Continued employment = acceptance

17. Final Declaration

All employees must comply strictly.

Non-compliance will result in:

Immediate disciplinary + legal action