

DATA PROTECTION, IT SYSTEMS AND INFORMATION PROCESS POLICY

1. Introduction

At Jain Metal Group ("JMG") we have always believed in sound, moral, ethical, and business principles. We are committed to act fairly with integrity and trust in all its business dealings and relationships wherever it operates.

The Data Protection, Information Technology ("IT") Systems and Information Process policy provides the general rules and guidelines to be followed while managing / handling the information / data for our material stakeholders – Customers, Vendors / Suppliers / Business Partners and Employees. The protection of company related data of our operations and daily affairs are part of our Business as Usual (BAU) and is aligned with our compliances, licence to operate and other regulatory laws and associated processes.

To be a responsible business group it is of utmost importance to uphold a high level of professional conduct in the business transactions of the Company which is consistent with our values and core purpose. This policy must be read in letter as well as in spirit.

2. Purpose

At JMG, we have always believed in sound, moral, ethical, and business principles and are committed to act fairly with integrity and trust in all our business dealings and relationships wherever we operates.

The Data Protection, IT Systems and Information Process Policy ('Policy') sets out essential steps for our Employees (as defined herein below in section Scope and Applicability, point 1) who must take to avoid being implicated for money laundering and to prevent involvement in any activity relating to bribery, facilitation payments, or corruption, even when the involvement may be un-intentional.

3. Scope and Applicability

- I. This Policy is applicable to all the employees working at all levels and grades including senior managers, officers, directors, other employees (whether permanent, fixed term or temporary), consultants, contractors, trainees, interns, seconded staff, casual workers and agency staff, agents, or any other person associated with the Company and such other persons, including those acting on behalf of the Company (collectively for the limited purpose of this Policy referred as 'Employees').
- II. This Policy governs all operations of JMG, whether domestic or international.
- III. This policy is to establish a Zero tolerance approach towards any malicious / deliberate intent to expose the company systems / assets / collaterals (digital / physical) to any harm or misuse by any unethical practices during interactions with



stakeholders (internal / external) providing or passing information through access which is not compliant to company laws / local laws and regulations.

- IV. Regardless of the territory or location of your work, undertaken on behalf of JMG, this Policy and all applicable data protection laws apply to you.
 - a. Digital personal data protection act 2023
 - b. Internal company defined systems and processes for IT – Data Security and Device Security.
 - c. ISO, Raid, Business Continuity Management - Framework / Plan (BCM / BCP)
- V. If any part of this Policy conflicts with local laws in any location, the local law of the appropriate jurisdiction will prevail. In case of queries or concerns you should get in touch with your respective Compliance Officer, as defined herein below.
- VI. Compliance Officer to ensure that the right Governance process is in place for the implementation and observance of this Policy ("Compliance Officer").

4. Personal Data Security

The company and its employees will maintain data of personal nature for limited use such as KYC and similar process post consent of the stakeholder. The data is to be used for lawful purposes which is communicated in a transparent manner and maintained as per regulatory guidelines concerning the use of personal data.

- **Customer:** (as per business and compliance requirements) KYC Data to be kept for a minimum of 1 year (accounting cycle) to a maximum of 5 years (audit and compliance purposes).
- **Vendor / Supplier / Business Partners:** (as per business and compliance requirements) Data to be kept for a minimum of 1 year (accounting cycle) to a maximum duration (till post contract 5 years for audit and compliance purposes) In case of important / essential items / machinery – life of the item till replaced by another vendor / product.
- **Employee:** (as per business and compliance requirements) KYC Data of employee for the duration of his / her tenure and completion of financial year (if exit is in the middle of the year) to a maximum of 5 years. In case of important / essential position or decision-making position then with permission of the employee retain till life of business / as official record.

5. Limitation in Use of Personal Data

The company and its employees will use the personal data of the stakeholders acquired post consent only for the purpose specified at the time of obtaining consent of the Data Principal. The use of the personal data will be governed by business ethics and code of conduct as established by the company for all its employees. (As detailed in scope and applicability point 1)



- **Customer:** KYC and any additional essential details – transaction related needed for an Audit compliance or Assessment by external vendors.
- **Vendors / Suppliers / Business Partners:** Data covering the essential details on the kind of transactions goods / services exchanges, warranty / guarantee if material is essential/critical needed for an Audit compliance or Assessment by external vendors or in case of an emergency / incident in relation to the said good / services – escalation and Immediate Response.
- **Employee:** KYC and any additional essential details – HR and Business related needed for an Audit compliance or Assessment by external vendors / stakeholders.

6. Use of Minimum Data

The company and its employees will acquire the personal data of the stakeholders to the minimum requirement post consent for the purpose specified at the time of obtaining consent of the Data Principal. The use and retention of stakeholder's data will be governed by business ethics and code of conduct as established by the company for all its employees. (As detailed in scope and applicability point 1).

- **Customers:** KYC Data to be kept for a minimum of 1 year (accounting cycle) to a maximum of 5 years (audit and compliance purposes) – scope to be defined as per business / services offered.
- **Vendor / Supplier / Business Partners:** Data to be kept for a minimum of 1 year (accounting cycle) to a maximum duration (till post contract 5 years for audit and compliance purposes) In case of important / essential items / machinery – life of the item till replaced by another vendor / product.
- **Employee:** KYC and any additional essential details – HR and Business related needed for an Audit compliance or Assessment by external vendors / stakeholders.

7. Data Accuracy

The company and its employees will acquire the personal data of the stakeholder as per the requirement post consent. However, the accuracy, completeness and validity of the data onus is on the stakeholders themselves. The company and its employees will not be adding or modifying the data for which is not the custodian.

- **Customers:** KYC Data to have supporting evidences – Aadhaar Card, Pan Card, and Bank Account details, to maintain data transparency and validation of business transaction being completed via verifiable channels.



- **Vendor / Supplier / Business Partners:** Vendor diligence, vendor management system – on-boarding (checks of compliance requirement).
- **Employee:** KYC and any additional essential details – HR and Business related needed for an Audit compliance or Assessment by external vendors / stakeholders.

8. Data Storage and Holding of Stakeholder Information

The company and its employees will acquire the personal data of the stakeholder as per the operational / compliance requirement post consent in its original form as received from the Data Principal. The records will be managed for a specific time period as per the rules and regulations laid down regarding user data and will be stored in a transparent and secure data environment / ecosystem.

- **Customers:** Limited information to be stored in premises or physical systems. For repeat customers switch from paper to digital data trail for storage online is recommended. Majority of information on servers / Cloud Based IT Systems with ISO Level Security with Business Continuity Plan.
- **Vendor / Supplier / Business Partners:** Limited information to be stored in premises or physical systems. Switch from paper to digital storage of invoices and transactions. Majority of information on servers / Cloud Based IT Systems with ISO Level Security with Business Continuity Plan.
- **Employee:** Emails, Meeting Notes, Laptops and any other official digital footprint to be synced with data protection and privacy eco-system to avoid / prevent / protect against data leaks or any other malicious use of company assets. ISO, Raid and BCP systems enabled with online data backup and recovery enabled IT devices. Any additional essential details – Business related to have a regular internal and external audit compliance or assessment by external vendors / stakeholders.

9. Data Security and Safeguards

The company and its employees will acquire and establish the necessary infrastructure to build an effective, resilient and reliable IT – ecosystem to manage and protect user data. The user data and information will include all the information which is accessed and used through the business journey in the operations and daily BAU. The BOD, company IT teams will establish the necessary protocols, Business Continuity Plans (BCP) and relevant systems with a certain degree of assurance to ensure safety of information based on a transparent and secure data environment / ecosystem.

- **Customers:** Access to customer data over a secured portal / application governed by strong data security systems – ISO Audited to keep customer data secure. Limited access post 2 / 3 level approvals for data extraction (by KMP or Process) and access only within company LAN / Domain and company assets.



- **Vendor / Supplier / Business Partners:** Vendor Access to systems on site governed by IT policies, systems and processes. Limited Access and within premises to essential data to be controlled – access by company owned and monitored assets. Majority of information on servers / Cloud Based IT Systems with ISO Level Security with Business Continuity Plan.
- **Employees:** Password Protection and regular updates to change and maintain minimum safety guidelines for password, IT Laptop security domain and ecosystem (VPN, LAN, Remote Access, and etc.), Online updates – system and security, access in safe internet connections to protect against data leaks or any other malicious use of company assets. ISO, Raid and BCP systems enabled with online data backup and recovery enabled IT devices.

10. Data Accountability, Breaches and Grievance Mechanisms

The company and its employees will acquire and establish the necessary systems and mechanism to prevent data loss, breaches and safeguard against internal, external leaks, hacks, fishing, malware, dark web leaks of stakeholder information which is part of company asset and collaterals. The IT ecosystem will have a layered security with clear and transparent chain of command and escalation matrix to deal with any incidents with a robust reporting and incident management mechanism. Business Continuity Plans (BCP) with relevant IT Protection systems to be implemented, assessed and monitored to provide assurance towards safety of data / information accessible in the company environment / ecosystem. Data leaks and breaches incident are managed as per established policies and security protocols with defined reporting mechanisms and collaboration with relevant stakeholders.

- **Customer:** Ownership of Customer data with Customer for applicability and completeness to establish accountability. Update in the case of changes – again with customer. Data of customer to be protected and uploaded over cloud systems for storage – security, limited access and ease of storage.
- **Vendor / Supplier / Business Partners:** Ownership of vendor data with vendor during the on-boarding process for applicability and completeness to establish accountability. Update in the case of changes – again with vendor. Data of vendor to be protected and uploaded over cloud systems for storage vendor management systems – security, limited access and ease of storage.
- **Employees:** Employee data over HRMS or company ecosystem. Employee data with employee for applicability and completeness to establish accountability. Update in the case of changes – again with employee. Data of employee with the IT and Company systems and processes example - Password Protection and regular updates to change and maintain minimum safety guidelines for password, IT Laptop security domain and ecosystem (VPN, LAN, Remote Access, etc.), Online updates – system and security, access in safe internet connections to protect against data leaks or any other malicious use of



company assets. ISO, Raid and BCP systems enabled with online data backup and recovery enabled IT devices.

11. Training and Capacity Building

To ensure that all Employees (as defined above), relevant independent directors, business partners, material third parties, are completely familiar to the provisions of this Policy and applicable regulations and guidelines / processes defined. The Group shall provide regular training for IT Security and Awareness on risks and prevention to avoid data leaks and data loss from internal and external resources as deemed appropriate and necessary to requirement.


12. Reporting and Escalation

Every Employee is encouraged to raise concerns about any data leaks or suspicion of malpractice or any case of corrupt practice with an intent to harm / cause loss of name in public / any breach of security by misuse / compromise of company assets this Policy or applicable regulations and guidelines / processes defined at the earliest possible stage. If he / she is unsure whether a particular act constitutes bribery or corruption or if he / she has any other queries, these should be raised with the Compliance Officer of the Company.

13. Responsibility and Penalties

JMG takes violations pertaining to data breaches, loss of data or deliberate attempt to sabotage assets or collaterals in digital / cause loss of reputation in public or social media seriously. Any non-compliance of this Policy will be regarded as a serious matter and shall result in disciplinary action, including termination, consistent with applicable law and defined Guidelines and Terms of Employment and review of the Compliance Officer / Committee.

For JAIN RESOURCE RECYCLING LIMITED


BIBHU KALYAN RAUT
Company Secretary

