JAI CORP LIMITED

Cyber Security & Data Privacy Policy

Cyber Security & Data Privacy Policy

Background/Preamble:

Jai Corp Limited (hereinafter referred to as "**the Company**" or "**Jai Corp**" or "**We**" or "**Our**" or "**Us**") is into manufacturing businesses such as plastic processing and steel. Jai Corp is committed to uphold the highest moral, legal, and ethical standards of cyber security and data privacy in all its business operations. This Policy is consistent with the Company's code of conduct and internal policies.

Purpose:

This policy aims to uphold privacy and protect the personal data of individuals associated with the Company, including employees, directors, senior executives, officers, consultants, contractors, trainees, suppliers, and the community. It ensures compliance with relevant laws and regulations governing data protection.

As an encompassing framework for information technology security, this Policy acknowledges the importance of privacy regulations and personal data protection standards. The Company recognizes that safeguarding individuals' data is vital to maintaining its reputation and preventing harm. The primary objective of this policy is to raise awareness about cyber security and data privacy, fostering a culture of vigilance throughout the organization.

Furthermore, this policy offers guidance on utilizing the available platforms within the Company to address any concerns related to cyber security. For reporting such concerns, individuals may contact the designated email address: sap@jaicorpindia.com.

Scope and Coverage:

This Policy applies to all individuals associated with the Company, including employees (whether permanent, fixed-term, or temporary), directors, senior executives, officers, consultants, contractors, trainees, workers, interns, business partners, suppliers, and members of the community. It covers those who have access to personal information collected or processed by the Company, as well as those who voluntarily provide information to the Company. These individuals are bound by the terms and conditions outlined in this Policy.

Definition:

"Policy" means "Cybersecurity Policy"

"Stakeholders" means and includes employees, workers, value-chain partners like suppliers, service providers, contractors, channel partners (including dealers), consultants, intermediaries like distributors and agents, lenders, customers, and business associates.

Cyber Security and Data Privacy Policy Statements:

The Company recognizes the importance of safeguarding personal and sensitive data, including information covered by regulatory provisions such as price sensitive information and details of complainants in cases related to discrimination or prevention of sexual harassment (POSH). It acknowledges the need for appropriate controls during the collection, transfer, storage, and processing of personal data, while ensuring compliance with applicable laws.

This policy outlines the responsibilities of all individuals affiliated with the Company to:

- Maintain the availability, integrity, and confidentiality of information.
- Manage the risks associated with security exposure or compromise.

…2/-

- Foster a reliable IT environment.
- Monitor systems for any anomalies that may indicate compromise, promptly responding to data breaches.
- Promote awareness of information security and enhance understanding among employees and other affiliates.

Additionally, this policy establishes a framework to ensure the implementation of necessary safeguards, preserving the confidentiality, integrity, and availability of data. It emphasizes the importance of educating employees and other affiliates about their roles, responsibilities, and the security policy, processes, and practices in place.

Responsibilities:

The Company has the following responsibilities:

1. Awareness and Training: Creating awareness and providing training on fundamental information security protocols necessary to protect the confidentiality, integrity, and availability of entrusted information.
2. Prevention of Misuse: Taking measures to prevent unauthorized parties from misusing resources or information.
3. Prevention of Illegal Use: Safeguarding sensitive and personal data to prevent its illegal use.
4. Reporting Incidents: Promptly reporting suspected information security incidents to the designated or dedicated incident reporting system.
5. Monitoring Cyber Security: Monitoring the performance of cyber security management systems, including the utilization of tools such as Securus.
6. Resource Provision: Providing resources to maintain information security controls consistent with this policy.
7. Risk Assessment and Audits: Conducting regular risk assessments and audits on its cyber security systems, both internally and through engagement with independent experts/agencies.

Grievance Redressal Mechanism:

All stakeholders, including those utilizing the Company's system, data terminals, or computer systems, are required to promptly report any security breaches or identify any suspicious activities, such as unauthorized access or improper system use. Incidents should be reported immediately to the IT office via email, phone, or through their supervisor/manager.

It is essential for all relevant stakeholders to be familiar with the grievance redressal mechanism concerning cyber security and data privacy. They should have a clear understanding of how to address concerns and seek resolution in such matters. The details related to raising the grievances has been clearly highlighted in the Grievance Redressal Policy.

Enforcement:

Any stakeholder found to have violated this policy shall be subject to disciplinary action as per the Company’s policy and regulatory guidance.

Review and Approval:

The Company’s top management has a strategic role in the full implementation of this Policy ensuring the involvement of all personnel and of those who collaborate with the Company, and in maintaining the consistency of their behavior with the values embodied in this Policy.

…3/-

Applicability:

This Policy, duly approved by the Board of Directors on 11th August.2023, shall be applicable with effect from the 11th day of August, 2023 and future amendments / modifications shall take effect from the date stated therein.

-*-*-*-