PRISM JOHNSON LIMITED
CIN: L26942TG1992PLC014033
Registered Office: 305, Laxmi Niwas Apartments, Ameerpet, Hyderabad – 500 016.
Corporate Office: “Rahejas”, Main Avenue, V. P. Road, Santacruz (West), Mumbai – 400 054.

January 07, 2026

Details	
Primary Owner	Prism Johnson Limited
Effective Date	07/01/2026
Version	V.1.0
Last review date	*[Applicable only in case of revision henceforth]*

Artificial Intelligence (AI) & Machine Learning (ML) Policy

1. Purpose

The purpose of this policy is to establish a clear governance framework for the responsible, ethical, secure, and effective adoption of Artificial Intelligence (AI) and Machine Learning (ML) across the organization. As a building materials manufacturing company, AI/ML will be leveraged to enhance operational efficiency, product quality, safety, sustainability, customer experience, and decision-making while ensuring compliance with legal, regulatory, and ethical standards.

2. Scope

This policy applies to:

- All employees, contractors, consultants, and third parties using or developing AI/ML solutions for the company
- All AI/ML systems, tools, models, and applications developed internally or procured from external vendors
- All business functions, including manufacturing operations, supply chain, quality control, maintenance, sales, finance, HR, and IT

3. Objectives of AI/ML Adoption

AI and ML initiatives shall aim to:

- Establish a responsible AI framework that governs the development, deployment, and use of AI tools.
- Ensure transparency, ethical standards, and data integrity in all AI-related activities.
- Maintain compliance with relevant legal, regulatory, and client requirements.

- Improve manufacturing efficiency, yield, and throughput
- Enhance product quality and reduce defects
- Optimize supply chain planning, inventory, and logistics
- Improve energy efficiency, sustainability, and waste reduction
- Support data-driven decision-making

4. Guiding Principles

All AI/ML initiatives must adhere to the following principles:

4.1 Ethical and Responsible Use

- AI/ML systems shall be designed and used in a fair, transparent, and accountable manner
- AI shall augment human decision-making and not fully replace critical human judgment, especially in safety-critical areas
- Outcomes must avoid bias, discrimination, or unfair treatment

4.2 Safety and Reliability

- AI/ML models used in manufacturing and operational environments must be tested, validated, and monitored to ensure accuracy and reliability
- Safety-related decisions must include human oversight

4.3 Core Principles

- **Transparency:** Users must disclose to their reporting managers when AI systems or outputs are being utilized. AI-generated content must be clearly acknowledged, particularly when shared with clients or colleagues.
- **Human-Centered Values:** Users must respect human rights, individual autonomy, and diversity, and should not replace human judgment in critical decisions.
- **Privacy and Security:** All AI users must respect confidentiality, data protection, and companies' & client's information security standards. No sensitive or proprietary information may be shared with AI tools without prior approval from the reporting manager.
- **Responsible Governance:** All AI-related activities must comply with the Company's ethical guidelines, regulatory requirements, and internal AI governance framework

4.4 Data Privacy and Security

- AI/ML systems must comply with applicable data protection and privacy laws
- Sensitive, proprietary, and personal data must be protected through appropriate security controls

4.5 Regulatory and Legal Compliance

- AI/ML usage must comply with all applicable laws, regulations, and industry standards
- Intellectual property rights must be respected when using external data, models, or tools

5. Prohibited and Restricted Uses

The following uses are prohibited or restricted:

- Fully autonomous decision-making in safety-critical operations without human oversight
- Use of AI for surveillance that violates employee privacy or labor laws
- Use of unapproved generative AI tools for sharing confidential or proprietary information
- AI applications that violate ethical standards, laws, or contractual obligations

6. Responsibility

Artificial Intelligence (AI) is everyone's responsibility in the Company.

The head of the departments/ verticals and process owners, from IT, Manufacturing, Sales, Marketing, HR, Legal, Risk, Finance and others will jointly:

- Approve AI/ML use cases and investments
- Define risk classification for AI systems (low, medium, high risk)
- Review ethical, legal, and operational risks
- Oversee policy compliance and periodic reviews

Roles and Responsibilities

- **Business Owners:** Define objectives, validate outcomes, and ensure responsible use
- **IT / Data Science Teams:** Develop, test, deploy, and maintain AI/ML models
- **Risk & Compliance**: Assess risks, regulatory compliance, and controls
- **Information Security**: Ensure data and system security
- **End Users:** Use AI tools responsibly and report issues or anomalies

7. Responsible Use Principle

- Users must ensure that any AI-generated output is obtained only through accounts or login credentials authorized for official, commercial work purposes, and not through personal or unauthorized access.
- All AI-assisted material must be reviewed by an employee before use. The reviewer (reporting manager) must ensure the content is factually correct, suitable for the intended audience, aligned with the Company's values, and free from bias or misleading information.
- Any use of AI in preparing documents, reports, presentations, or communication should be transparently acknowledged wherever relevant.
- Employees must understand that AI tools may generate outdated, inaccurate, or fabricated information and therefore human verification is mandatory before relying on any output.
- Exercise caution with every piece of data shared with AI platforms. Treat inputs as if they could become publicly visible and attributed to you or the Company.
- Employees should inform their reporting manager whenever AI tools are used to support the completion of significant tasks or deliverables.
- Before applying or sharing AI-generated output, employees must validate that the content does not infringe intellectual property rights, violate privacy regulations, introduce workplace bias, or breach Company policies.

8. Data Management Standards

- Data used for AI/ML must be accurate, relevant, and obtained from authorized sources
- Data quality checks, lineage, and version control must be maintained
- Training data must be periodically reviewed to prevent bias or degradation

9. Model Development, Testing, and Deployment

- All AI/ML models must follow a defined development lifecycle including:
  - Business requirement definition
  - Data preparation and validation
  - Model training and testing
  - Performance and bias evaluation
  - Approval prior to production deployment
- Changes to models must follow formal change management processes

10. Monitoring and Performance Management

- AI/ML models must be continuously monitored for performance, accuracy, and drift
- KPIs and thresholds must be defined for each model
- Material issues must be escalated and remediated promptly

11. Vendor and Third-Party AI

- Third-party AI solutions must undergo due diligence covering security, privacy, IP rights, and compliance
- Contracts must clearly define data ownership, usage rights, and responsibilities

12. Training and Awareness

- Employees involved in AI/ML initiatives must receive appropriate training
- Awareness programs shall be conducted to promote responsible and secure AI usage

13. Incident Management

- AI-related incidents (data breaches, model failures, safety issues) must be reported and managed through the company's incident management process
- Root cause analysis and corrective actions must be documented

14. Policy Review and Updates

This policy shall be reviewed annually or upon significant changes in technology, regulation, or business strategy.

15. Non-Compliance

All violations of security policies, standards and/or guidelines are subject to disciplinary action.

The specific disciplinary action depends upon the nature of the violation, the impact of the violation on informational assets and related facilities, etc. Violations will be handled as per the existing HR processes and could range from verbal reprimand to termination of employment/contract and/or legal action.

If a department or function is unable to comply with any requirements detailed within this policy, an exception shall be obtained. Such exceptions shall be documented and approved by the management team in Enterprise Risk Management meeting indicating the rationale for the exception and the related risks.

16. Policy Revision

This policy will be periodically reviewed in order to ensure its continued adequacy and relevance. It may be amended at any time with the approval of the Chief Financial Officer (CFO) of the Company.