POLICY ON CYBER SECURITY AND RISKS RELATED TO DATA PRIVACY

1. SCOPE AND PURPOSE

Kalyan Jewellers India Limited ("the Company") is committed to safeguarding the confidentiality, integrity, and availability of its digital assets, customer data, and information systems. This Cyber Security and Data Privacy Risk Management Policy seeks to establish a robust framework for securing the Company's IT infrastructure and digital operations, ensuring regulatory compliance and reinforcing stakeholder trust.

This Policy applies to:

- All business units and functions of **Kalyan Jewellers India Limited**, including its **domestic and international subsidiaries**;
- **Employees, consultants, contractors, and third-party service providers** who have access to the Company's IT systems, customer data, or any confidential information;
- **Digital platforms**, including e-commerce, mobile applications, ERP systems, cloud storage, internal tools, and social media channels operated by the Company.

2. Cyber Security Vision

The Company's vision is to remain resilient, secure, and agile in the face of evolving cyber threats, data breaches, and digital vulnerabilities. It is committed to protecting all sensitive business information, including the personal data of customers, employees, and business partners, while fostering a culture of security awareness and responsibility across all levels of the organization.

3. Security Policy

1. **Protection of Information and Assets:** Implementing robust security controls to prevent unauthorised access, covering physical, logical, and personnel security.
2. **Compliance:** Adhering to legal and regulatory requirements across all our operations.
3. **Business Continuity:** Ensuring continuity of operations in line with business requirements and obligations to our stakeholders.
4. **Security Responsibilities:** Defining and assigning specific security responsibilities to departments and individuals to ensure adherence to this policy.

5. **Security Awareness and Competence:** Promoting adequate security awareness and building competence among all associates to fulfill their responsibilities .
6. **Reporting Mechanisms:** Providing secure channels for associates and stakeholders to report security weaknesses, violations, or disruptions of service.
7. **Response Framework:** Establishing a robust framework to handle security weaknesses, violations, or disruptions of services.
8. **Governance:** Monitoring security performance against targets and objectives, enabling continuous improvements.

4. **Enforcement and Disciplinary Action**

Any violations of this Policy shall lead to disciplinary action, which may include termination of employment or engagement and potential legal action. The same applies to third-party vendors found non-compliant with the Company's cyber security and data privacy requirements.

5. **Policy Review and Updates**

This Policy shall be reviewed annually or in response to significant changes in applicable regulations, technology, or cyber threat landscape. Updates shall be approved by the Board or its designated Committee.