(HI KLASS TRADING AND INVESTMENT LIMITED)

CYBER SECURITY POLICY

(Adopted by the Board of Directors of the Company at their meeting held on 13TH
February 13, 2026

INTRODUCTION

Hi Klass Trading and Investment Limited (the 'Company'), is a registered NBFC carrying on the business of financing and investment activities by way of advancing Inter-Corporate Deposits and acquisition of shares and securities of its group companies.

According to the directions issued by the Reserve Bank of India (RBI) in this regard, the following Cyber Security Policy ('Policy') has been formulated and adopted by the Board of Directors of the Company. This Policy outlines the guidelines, procedures, and best practices to ensure the security of information systems, data assets, and digital operations within the company. The Policy aims to safeguard against cyber threats, protect customer information, and maintain business continuity.

SCOPE

This Policy applies to all employees, contractors, vendors, and third-party service providers who have access to Company systems, networks, and data assets.

GOVERNANCE AND COMPLIANCE

- ***Responsibilities:*** The Chief Information Security Officer (CISO) or equivalent executive will oversee the implementation and enforcement of this Policy. All employees are responsible for adhering to the Policy and reporting any cybersecurity incidents promptly.
- ***Compliance:*** The Company will comply with all applicable laws, regulations, and industry standards related to cybersecurity, including but not limited to data protection laws and regulatory requirements specific to NBFCs.

INFORMATION SECURITY CONTROLS

Access Control: Access to systems, networks, and data assets will be granted on a need-to-know basis. User access privileges will be regularly reviewed and updated as per job roles and responsibilities.
Authentication: Multi-factor authentication (MFA) will be enforced for accessing critical systems and applications, especially for remote access and privileged accounts.

Data Encryption: All sensitive data, both at rest and in transit, will be encrypted using industry-standard encryption algorithms to prevent unauthorized access or interception.

Network Security: Firewalls, intrusion detection and prevention systems (IDPS), and other network security measures will be implemented to detect and mitigate unauthorized access and malicious activities.

Endpoint Security: Endpoint protection solutions, including antivirus software, endpoint detection and response (EDR) tools, and mobile device management (MDM) solutions, will be deployed to secure end-user devices.

INCIDENT RESPONSE AND MANAGEMENT

Reporting: Employees must promptly report any cybersecurity incidents, including but not limited to data breaches, malware infections, and suspicious activities, to the IT or security team.

Response Plan: The Company will maintain an incident response plan outlining the procedures for identifying, containing, mitigating, and recovering from cybersecurity incidents. The plan will be regularly tested and updated as necessary.

Notification: In the event of a data breach or security incident involving customer information, the Company will comply with legal and regulatory requirements for notifying affected individuals, regulatory authorities, and other stakeholders.

EMPLOYEE AWARENESS AND TRAINING

Training Programs: The Company will conduct regular cybersecurity awareness training sessions for all employees to educate them about cybersecurity risks, best practices, and their roles and responsibilities in maintaining security.

Phishing Awareness: Employees will receive training on identifying and reporting phishing attempts, social engineering attacks, and other forms of cyber threats.

THIRD-PARTY RISK MANAGEMENT

Vendor Security Assessment: The Company will assess the cybersecurity posture of third-party vendors and service providers before engaging in business relationships. Contracts with vendors will include provisions for cybersecurity requirements and responsibilities.

Monitoring and Oversight: Ongoing monitoring of third-party vendors' security practices and compliance with contractual obligations will be conducted to mitigate risks associated with outsourcing.

SECURITY INCIDENT REPORTING AND REVIEW

Incident Reporting: All cybersecurity incidents, including near misses and potential vulnerabilities, will be documented and reported to the CISO or designated security officer for review and analysis.

Post-Incident Review: After the resolution of cybersecurity incidents, a thorough post-incident review will be conducted to identify root causes, lessons learned, and areas for improvement in the Company's cybersecurity defenses and incident response procedures.

REVIEW OF THE POLICY

The Policy shall be amended and modified with approval of the Board. The Board of Directors of the Company shall monitor and review the Policy on an Annual basis. Any Amendments in RBI guidelines or any change in the position of the Company, necessary changes in this Policy shall be incorporated and approved by the Board. The Policy is reviewed and recommended by the Audit Committee at its meeting held on 13th February 2026, approved by Board of Directors at its meeting held on 13.02.2026

CONTACT INFORMATION

For any questions, concerns, or reporting of cybersecurity incidents, employees may contact:

Name of the person: Neha Kedia
Designation: Company Secretary
Email ID: info@hiklass.co.in
Contact No.: 9874385558