MUFIN GREEN FINANCE LIMITED

Information Security Policy

V.03 | Document Number: MGFL/ISP/POL/01

DOCUMENT CONTROL:

Policy / Document Title	Information Security Policy
Applicable To	Mufin Green Finance Limited ("MGFL" / "the Company")
Current Version	V.03
Current Status	Final
Current Effective Date	02nd September, 2026
Next Review Date	01st September, 2027
Document Owner	Mr. Amit Sharma and Mr. Manoj Taneja

VERSION & APPROVAL HISTORY:

Version	Created / Revised By	Reviewed By	Approved By	Approval Date	Effective Date	Change Description
V.01	Mr. Mayank Pratap Singh	-	Board of Directors	01st September, 2022	01st September, 2022	Initial version
V.02	Mr. Deepak Bansal		Board of Directors	14th February, 2024	14th February, 2024	Amended pursuant to RBI Master Direction – Information Technology Framework and RBI Information Technology Directions, 2023
V.03	Mr. Subhash Kanagaraj	Mr. Amit Sharma and Mr. Manoj Taneja	Board of Directors (on the recommendation of IT Strategy Committee)	02nd September, 2026	02nd September, 2026	Amended pursuant to RBI (NBFC – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026.

Table of Contents

1. Introduction 4
2. Objective....4
3. Applicability 4
4. Regulatory Framework....5
5. Definitions 5
6. Information Security Governance Structure....6
- ❖ Board of Directors 6
- ❖ IT Strategy Committee (ITSC)....6
- ❖ Information Security Committee (ISC) 6
- ❖ Chief Information Security Officer (CISO)....6
- ❖ IT Steering Committee 7
- ❖ Audit Committee of the Board (ACB) 7

7. Policy Statement....7
7.1 Commitment and Compliance 7
7.2 Risk Management and Asset Management....7
7.3 Technology and Network Controls....7
7.4 Application Security and Logging 8
7.5 Access Control and Secure Working Practices....8
7.6 Third-Party and Outsourcing Risk Management 8
7.7 Continuous Surveillance and Threat Defence....8
7.8 Testing, Assurance and Resilience....9
7.9 Incident Response, Reporting and Awareness....9
8. Policy Compliance....10
- ❖ Compliance Measurement....10
- ❖ Exceptions 10
- ❖ Non-Compliance....10

9. Information Systems (IS) Audit 10
10. Disclaimer....10
11. Consequence Management and Non-Compliance....11
20. Regulatory Compliance and Precedence 11
21. Policy Review....11

1. Introduction

Mufin Green Finance Limited ("Mufin" or "the Company") is a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India (RBI) and recognizes that protecting information is fundamental to maintaining customer and stakeholder trust, ensuring regulatory compliance, and sustaining safe and sound financial operations. As a regulated financial entity, Mufin handles sensitive customer financial data, loan and credit information, KYC records, and payment data, making information security a core element of its risk management and corporate governance framework.

This Information Security Policy ("Policy") establishes Mufin's commitment to implementing a robust and comprehensive framework for the protection of all information assets, including customer and borrower data, financial records, intellectual property, employee records, and operational information. It serves as a guiding document for the Board of Directors, employees, contractors, consultants, and third-party service providers, defining the principles, objectives, and controls required to ensure the confidentiality, integrity, and availability of information, in line with RBI directions applicable to NBFCs.

2. Objective

The objectives of the Information Security Policy at Mufin Green Finance Limited are to:

- **Protect Information Assets:** Safeguard the confidentiality, integrity, and availability of all information, including customer and borrower data, financial and credit information, intellectual property, and operational records.
- **Manage Risks:** Identify, evaluate, and mitigate information security and cyber risks through proactive controls, continuous monitoring, and periodic risk assessments as envisaged under RBI's Cybersecurity, Technology: Risk, Resilience and Assurance Framework Directions, 2026.
- **Ensure Regulatory Compliance:** Adhere to applicable RBI directions and guidelines, and other legal, regulatory, and contractual obligations relating to data protection and information security.
- **Enable Incident Response:** Maintain an effective framework to detect, respond to, and recover from cyber security incidents with minimal impact, including timely reporting to the RBI and other regulators as mandated.
- **Promote Awareness:** Foster a culture of security through regular training, communication, and accountability across the Board, management, and staff.
- **Control Access:** Enforce strict access management aligned with the principle of least privilege and business need-to-know, particularly for systems processing customer financial data.
- **Ensure Business Continuity:** Maintain resilience of critical customer-facing and financial operations through robust business continuity and disaster recovery arrangements.
- **Drive Continuous Improvement:** Review and enhance policies, controls, and practices to address emerging threats, technologies, and evolving RBI/regulatory requirements.

3. Applicability

This policy applies to all individuals and entities who access, process, or manage information assets of Mufin Green Finance Limited, across all branches, offices, and business correspondent/agent locations.

This includes, but is not limited to:

- Board of Directors and Senior Management
- Full-time and part-time employees
- Contractors and consultants
- Interns and freelancers
- Third-party service providers, IT/technology vendors, and outsourcing partners
- Business correspondents, direct selling agents, and channel partners with access to Mufin's systems or customer data

All such personnel and entities are required to comply with the provisions of this policy and ensure that information assets, particularly customer and financial data, are handled responsibly and securely at all times.

4. Regulatory Framework

As an RBI-regulated NBFC, Mufin Green Finance Limited shall design, implement, and maintain its information security controls with reference to the following (as applicable to its Scale-Based Regulation layer, and as amended from time to time):

- RBI (Non-Banking Financial Companies– Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026: adopted voluntarily by Mufin as a benchmark for governance structures, baseline cybersecurity controls, CSOC capability, incident-reporting timelines, VA/PT periodicity, and BCP/DR practices, notwithstanding that these Directions are not directly applicable to NBFCs
- Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025 (as amended from time to time).Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025.
- RBI Master Direction on Know Your Customer (KYC)-2025 (as amended from time to time), for protection of customer identification data.
- The Digital Personal Data Protection Act, 2023 (DPDP Act) and DPDP Rules 2025 thereunder.
- The Information Technology Act, 2000 and rules made thereunder, including CERT-In cyber security directions.
- Prevention of Money Laundering Act (PMLA), 2002 & PMLA Rules 2005, to the extent relevant to data handling and reporting.
- Any other circular, direction, or guideline issued by the RBI, CERT-In, or other regulators concerning information and cyber security, as applicable to Mufin from time to time.

In the event of any conflict between this Policy and applicable RBI directions or law, the RBI directions/applicable law shall prevail, and this Policy shall be read and implemented accordingly.

5. Definitions

For the purposes of this Policy, and consistent with the FSB Cyber Lexicon and RBI usage, the following terms shall bear the meanings given below:

- Cyber Incident: A cyber event that adversely affects the cybersecurity of an information asset, whether resulting from malicious activity or not.
- Cyber Resilience: The ability of Mufin to continue to carry out its mission by anticipating and adapting to cyber threats and by withstanding, containing, and rapidly recovering from cyber incidents.
- Cybersecurity: Preservation of the confidentiality, integrity, and availability of information and information systems through the cyber medium.
- Vulnerability: A weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.
- Vulnerability Assessment (VA): Systematic examination of an information system to identify security deficiencies and confirm the adequacy of security measures.
- Penetration Testing (PT): A test methodology in which assessors, working under specific constraints, attempt to circumvent or defeat the security features of an information system.
- Red Team / Red Teaming Exercise: A simulated, real-world adversarial exercise conducted to assess the security capability of Mufin's information systems and organisation.
- Privileged User: A user who, by virtue of function or role, has been allocated system access rights significantly greater than those available to the majority of users.
- Recovery Time Objective (RTO): The maximum acceptable length of time an information system can remain in the recovery phase before negatively impacting Mufin's operations.
- Recovery Point Objective (RPO): The point in time to which data must be recovered after a disruption.

- Indicators of Compromise (IOCs): Identifying signs that a cyber incident may have occurred or may be currently occurring.
- Cyber Crisis Management Plan (CCMP): Mufin's documented plan addressing detection, containment, response, and recovery in relation to cyber-attacks and intrusions.

6. Information Security Governance Structure

In line with RBI's IT Governance, Risk, Controls and Assurance Practices Directions, Mufin shall maintain the following governance structure for information and cyber security oversight:

❖ Board of Directors

The Board of Directors holds ultimate responsibility and accountability for information security and cyber resilience. The Board shall approve this Policy, review it at least annually, and oversee the Company's overall cyber risk appetite and IT strategy.

❖ IT Strategy Committee (ITSC)

A Board-level IT Strategy Committee shall provide strategic oversight on IT investments, IT and cybersecurity risk management, and alignment of technology with business objectives. Consistent with leading practice for the ITSC's composition and conduct, Mufin shall ensure, to the extent commensurate with its scale:

- The ITSC comprises a minimum of three directors, including its Chairperson.
- The Chairperson is, where feasible, an independent director with substantial IT/cybersecurity experience.
- Members possess the ability to understand and evaluate information systems and associated IT/cyber risks.
- The ITSC meets at least quarterly and reviews IT strategy, budgetary adequacy, risk management processes, BCP/DR adequacy (at least annually), IT capacity assessments, and access administration standards.

❖ Information Security Committee (ISC)

A management-level Information Security Committee shall operate under the oversight of the ITSC and shall be responsible for development and implementation of information security/cybersecurity policies and standards, approval and monitoring of security projects and awareness initiatives, review of cyber incidents and IS audit observations, and periodic reporting to the ITSC and the Managing Director/CEO. Consistent with segregation-of-duties principles, the head of the ISC shall be drawn from the risk management vertical, with the CISO and representatives from business, IT, and other relevant functions as members.

❖ Chief Information Security Officer (CISO)

The CISO shall be a sufficiently senior executive responsible for the day-to-day management of information and cyber security, independent of IT operations. To maintain independence:

- The CISO shall have no direct reporting relationship with the Head of IT Function and shall not be assigned business targets.
- The CISO shall report to the Executive Director, or an equivalent executive overseeing the risk management function.
- The CISO shall be a permanent invitee to the ITSC and the IT Steering Committee, and shall place a review of cybersecurity risks, arrangements, and preparedness before the Board/ITSC at least quarterly.
- The CISO's office shall manage and monitor the Security Operations Centre, drive cybersecurity projects, and coordinate information security matters with relevant external agencies, including CERT-In.

❖ **IT Steering Committee**
An IT Steering Committee comprising senior management from IT and business functions shall meet at least quarterly to assist the ITSC in strategic IT planning, oversee business continuity and DR processes, ensure implementation of a compliant IT architecture, and update the ITSC and MD/CEO on its activities.

❖ **Audit Committee of the Board (ACB)**
The ACB shall exercise oversight of Information Systems (IS) Audit, approve the IS Audit Policy at least annually, and review critical IT/information security/cybersecurity issues raised by internal or external audit, providing direction to management as appropriate.

7. Policy Statement

7.1 Commitment and Compliance

- **Commitment to Information Security:** Mufin is committed to protecting the confidentiality, integrity, and availability of its information assets, with particular emphasis on customer financial data, credit information, and KYC records.
- **Compliance with Legal and Regulatory Requirements:** Mufin will comply with all applicable RBI directions and other laws, including the DPDP Act, the Information Technology Act, 2000, and, where applicable, the GDPR.

7.2 Risk Management and Asset Management

- **IT and Information Security Risk Management:** Mufin will maintain an IT and information security risk management framework, including periodic risk assessments, vulnerability assessments, and penetration testing of critical systems, reviewed and updated at least annually.
- **Inventory and Classification of Information Assets:** All information assets, including data, systems, hardware, software, and documents, will be inventoried and classified based on sensitivity and business criticality, with special categorization for customer financial and KYC data. An enterprise data dictionary shall be maintained to promote a common understanding of data across applications.
- **Data Leak Prevention:** Mufin will implement a data loss/leakage prevention strategy covering data at endpoints, in transmission, and at rest, including at vendor-managed facilities, and shall implement controls for remote wipe/lock of mobile devices and laptops.
- **Data Migration Controls:** Data migration activities will follow a documented process ensuring data integrity, completeness, and consistency, with audit trails and business/application-owner sign-off at each stage.

7.3 Technology and Network Controls

- **Software Control and Patch Management:** Mufin will maintain a centralised inventory of authorised/unauthorised software, control installation of software across endpoints, servers, and cloud environments, and apply security patches — including emergency patches for actively exploited vulnerabilities — in a timely, risk-based manner.
- **Secure Configuration:** Baseline security configurations will be documented and applied to endpoints, servers, databases, applications, and network/security devices throughout their lifecycle, and reviewed periodically.
- **Network Management and Security:** Network access will be authorised, time-bound, and audited. Mufin will maintain an up-to-date network architecture diagram and device inventory, secure wireless networks, and deploy multi-layered boundary defences (firewalls, DMZ, IPS/IDS) with real-time traffic filtering.
- **Physical and Environmental Controls:** Data Centre and Disaster Recovery sites will be protected against natural and man-made threats, geographically separated, and subject to e-surveillance and environmental-breach monitoring (temperature, water, smoke, power, access).

- **Capacity Management:** IT capacity requirements will be assessed at least annually against past usage trends, current needs, and the IT strategy.

7.4 Application Security and Logging

- **Application Security Life Cycle:** Information security will be embedded across the application life cycle, including secure coding practices, threat modelling, defence-in-depth, and security testing benchmarked against recognised standards such as OWASP (not limited to the OWASP Top 10). Development, test, and production environments will be segregated, and source code/escrow arrangements maintained for critical applications.
- **Audit Logs:** Every application or system handling critical or sensitive information will maintain audit trails sufficient to support audits, forensic investigation, dispute resolution, and non-repudiation. Logs will be regularly monitored to detect unauthorised activity.
- **Patch, Vulnerability, and Change Management:** Changes and patches will be assessed for business impact, approved, tested, and implemented through a documented, risk-based change management process, with a mechanism to recover from failed changes.

7.5 Access Control and Secure Working Practices

- **User Access Control:** Access to information systems and data, particularly core lending/financial systems, will be granted only on a valid business need and least-privilege basis. Administrative rights on end-user devices will be restricted, dormant accounts deactivated, invalid logon attempts controlled, and abnormal logon patterns monitored. Multi-factor authentication will be implemented for privileged users and for access to critical systems, based on risk assessment.
- **Controls on Teleworking:** Remote access to Mufin's environment will require secure systems, multi-factor authentication for critical systems, identification of all remote-access devices, and appropriate protection of data shared in teleworking.
- **Authentication Framework for Customers:** Mufin will implement an authentication framework enabling positive identity verification of customers and allowing customers to verify Mufin's authenticity across delivery channels.
- **Secure Mail and Messaging:** Mufin will implement measures to prevent email spoofing and look-alike domain abuse, filter malicious attachments and spam, and implement DMARC for its email domains, extending similar expectations to vendors and partners.
- **Removable Media:** As a default rule, removable devices and media will not be permitted unless specifically authorised for defined use and duration, scanned for malware before use, and subject to secure data erasure after use.
- **Cryptographic Controls:** Sensitive information, including customer financial and personal data, will be encrypted at rest and in transit using strong, internationally accepted, non-deprecated algorithms, protocols, and key lengths, with proper key management.

7.6 Third-Party and Outsourcing Risk Management

- **Third-Party Security and Outsourcing Risk Management:** When engaging IT/technology vendors, fintech partners, business correspondents, and outsourcing partners, Mufin will conduct vendor risk assessments proportionate to materiality, address concentration and single-point-of-failure risks, build appropriate security requirements into contracts (including right to audit by Mufin and, where applicable, by RBI or its authorised representatives), and perform ongoing due diligence and periodic audits, including background checks and confidentiality undertakings for personnel accessing critical assets.

7.7 Continuous Surveillance and Threat Defence

- **Continuous Surveillance – Security Operations Centre:** Mufin will maintain a Security Operations Centre (SOC) capability, commensurate with its scale, for continuous monitoring of security events using SIEM tooling, log correlation, and dashboards, with defined escalation for

anomalies, and appropriately skilled staffing for round-the-clock monitoring, incident investigation, and forensic support.

- **Advanced Real-Time Threat Defence:** Mufin will deploy anti-malware and antivirus protection with behavioural detection capabilities across endpoints, servers, gateways, and wireless networks, with centralised management and monitoring, and website/system whitelisting where appropriate.
- **Anti-Phishing:** Mufin will subscribe to anti-phishing/anti-rogue-application services to identify and take down phishing sites and rogue applications impersonating Mufin.

7.8 Testing, Assurance and Resilience

- **Vulnerability Assessment and Penetration Testing:** Mufin will periodically conduct VA and PT of critical and internet-facing systems, applications, servers, and network components, throughout their lifecycle. For critical/customer-facing systems, VA will be conducted at least every six months and PT at least annually, by independent, appropriately qualified auditors, with identified vulnerabilities remediated in a time-bound manner and status reported to the ISC/ITSC at least quarterly.
- **Red Teaming Exercises:** Mufin may conduct periodic red teaming exercises, commensurate with its risk profile, to assess the efficacy of its defences by simulating real-world adversarial behaviour.
- **Business Continuity and Disaster Recovery:** Information security requirements will be embedded in Business Continuity Plans (BCP) and Disaster Recovery (DR) arrangements, adopting good practices such as ISO 22301. For critical systems, DR drills will be conducted at least half-yearly, targeting minimal RTO and near-zero RPO, with DC and DR configurations and patch levels kept identical and backup data periodically tested for usability and integrity.
- **Straight Through Processing:** For critical applications, Mufin will avoid manual intervention in data transferred between processes/applications, using tested, securely automated, and audited data-transfer mechanisms.

7.9 Incident Response, Reporting and Awareness

- **Cyber Security Incident Response, Recovery, and Reporting:** Mufin will maintain a cyber incident response and recovery management policy covering incident classification, roles and responsibilities, reporting channels for employees/vendors/customers, communication strategy, containment and recovery measures, threat-information sharing, and post-incident review. All personnel are required to report security incidents immediately. Cyber security incidents shall be reported to the RBI and to CERT-In within the timelines prescribed under applicable directions (currently six hours of detection for CERT-In reporting).
- **Cyber Crisis Management Plan (CCMP):** Mufin will maintain a Board-approved CCMP addressing Detection, Containment, Response, and Recovery, covering threats such as DDoS, ransomware, destructive malware, and phishing/social-engineering-based fraud, including zero-day and targeted attack scenarios.
- **Metrics:** Mufin will develop and monitor key performance and key risk indicators — such as anti-malware coverage, patch latency, vulnerability metrics, and user-awareness levels — together with recovery metrics (RPO/RTO) for critical systems, and an overall IT/security maturity scorecard.
- **Training and Awareness:** Mufin will provide ongoing information security and cyber hygiene training for the Board, management, and all employees, mandatory for new recruits and refreshed at least annually, to build the ability to recognize and respond to threats such as phishing and social engineering.
- **Customer Data Protection and Customer Awareness:** Mufin will implement technical and organizational measures to protect customer, borrower, and KYC data, and will proactively educate customers on phishing reporting and the risks of sharing login credentials, passwords, OTPs, and PINs.
- **Risk-Based Transaction Monitoring:** Mufin will implement risk-based transaction monitoring/surveillance as part of its fraud risk management system across all delivery channels.

- **Digital Forensics:** Mufin will maintain (directly or through standby arrangements) network forensics, forensic investigation, and DDoS mitigation support to enable prompt root-cause analysis of incidents.
- **Continuous Improvement:** The Information Security Committee will regularly review and update this Policy and related procedures to reflect changes in the business environment, emerging cyber threats, technology developments, and evolving regulatory requirements.

8. Policy Compliance

❖ **Compliance Measurement**

The Information Security Team will verify adherence to this policy through multiple methods, including but not limited to:

- Periodic walk-throughs and inspections of branches, offices, and data centres.
- Review of business tool reports, system logs, and security monitoring alerts.
- Internal and external audits, including periodic IS Audit as expected under RBI directions.
- Feedback provided to the policy owner, CISO, and management.

❖ **Exceptions**

- Exceptions shall not be universal and will be evaluated on a case-by-case basis upon formal request by the information owner.
- Exceptions may arise due to business needs, local circumstances, legal or regulatory requirements, or other specific conditions. These may be temporary or permanent in nature.
- All exceptions must follow the organization's Exception Management Policy and be formally documented, with associated risk clearly articulated.
- The Chief Information Security Officer (CISO) shall review all exceptions at least annually to determine their continued validity and necessity, and material exceptions shall be reported to the Information Security Committee/ITSC.

❖ **Non-Compliance**

Employees, contractors, or third parties found in violation of this policy may be subject to disciplinary action, up to and including termination of employment, contract penalties, or legal action, depending on the severity of the breach. Where a violation results in a regulatory reporting obligation, the matter shall also be escalated to the CISO and Senior Management for appropriate reporting to the RBI or other regulators.

9. Information Systems (IS) Audit

Mufin will conduct periodic Information System audits of its IT infrastructure, applications, and security controls, commensurate with its risk profile and regulatory expectations. The ACB shall approve and review the IS Audit Policy at least annually, and shall review audit findings and remediation status. IS Audit planning shall follow a risk-based approach, and Mufin shall, wherever possible, consider a continuous auditing approach for critical systems. Where external resources are used for IS audit, responsibility and accountability shall remain with the competent authority within the Internal Audit function.

10. Disclaimer

Mufin Green Finance Limited reserves all rights and is the exclusive owner of all intellectual property rights over this document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDs, DVDs), and/or captured or transmitted through any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the CISO. The document is meant to be published on the intranet

of Mufin Green Finance Limited and/or any other forum as decided by the management of Mufin. Anything not specifically stated in this document shall not be considered as implied in any manner.
For any clarifications related to this document with respect to its interpretation, applicability, and implementation, please write to the CISO.

11. Consequence Management and Non-Compliance

All violations of this policy, standard 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, and any resulting regulatory implications. Violations will be handled as per the existing HR processes and could range from a 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, indicating the rationale for the exception and the related risks. Exceptions to this policy shall follow the exception process for prior authorization and approval.

20. Regulatory Compliance and Precedence

In the event of any conflict or inconsistency between the provisions of this Policy and the applicable laws, rules, regulations, notifications, circulars or directions issued by the Reserve Bank of India (RBI) or any other competent authority, the provisions of the applicable law or regulatory requirements shall prevail.

21. Policy Review

This Policy shall be reviewed periodically, and at least once every year, or earlier, if required due to any change in applicable laws, regulations, RBI Directions or the business requirements of the Company. Any amendments to the Policy shall be placed before the appropriate authority for review and approval.

****