MUFIN GREEN FINANCE LIMITED

Information & Cyber Security Risk Management Policy

Version 1.0

DOCUMENT CONTROL:

Policy / Document Title	Information & Cyber Security Risk Management Policy
Applicable To	Mufin Green Finance Limited ("MGFL" / "the Company")
Current Version	V.01
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. 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	Initial version - Adoption pursuant to RBI (NBFC – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026.

Table of Contents

1. Introduction, Objective and Guiding Principles 5
1.1 Background 5
1.2 Objective 5
1.3 Guiding Principles 5
2. Scope and Applicability 5
3. Definitions 6
4. Governance Structure and Roles 6
4.1 Board of Directors 6
4.2 IT Strategy Committee (ITSC) 6
4.3 IT Steering Committee 7
4.4 Information Security Committee (ISC) 7
4.5 Chief Information Security Officer (CISO) 7
5. IT and Information Security Risk Management Framework 7
5.1 Periodic Review 7
5.2 Framework Components 7
5.3 Risk Identification, Assessment and Documentation 8
6. Baseline Cybersecurity and Resilience Requirements 8
A. Inventory Management of Information Assets 8
B. Data Leak Prevention (DLP) 8
C. Data Migration Controls 8
D. Preventing Execution of Unauthorised Software 8
E. Physical and Environmental Controls 8
F. Capacity Management 9
G. Secure Configuration 9
H. Network Management and Security 9
I. Application Security Lifecycle 9
J. Maintenance, Monitoring and Analysis of Audit Logs 9
K. Patch, Vulnerability and Change Management 9
L. User Access Control / Management 10
M. Controls on Teleworking / Work-from-Home 10
N. Authentication Framework for Customers 10
O. Secure Mail and Messaging Systems 10
P. Removable Media 10
Q. Third-Party / Vendor Arrangements 10

R. Cryptographic Controls 10
S. Straight Through Processing (STP) 11
T. Continuous Surveillance / Cyber Security Operations Centre (CSOC) 11
U. Advanced Real-Time Threat Defence and Management 11
V. Anti-Phishing 11
W. Vulnerability Assessment and Penetration Testing (VA/PT) 11
X. Red Teaming Exercises 11
Y. Business Continuity Planning (BCP) and Disaster Recovery (DR) 11
Z. Cyber Incident Response and Recovery Management 11
AA. Metrics 12
BB. User / Employee / Management Awareness 12
CC. Customer Education and Awareness 12
DD. Risk-Based Transaction Monitoring 12
EE. Forensics 12
7. Cyber Security Operations Centre (CSOC) 12
7.1 Governance 12
7.2 Capabilities 12
7.3 Staff Capabilities 13
8. Information Systems (IS) Audit 13
9. Departmental Roles and Responsibilities 13
10. Exceptions, Non-Compliance and Policy Enforcement 14
11. Policy Compliance 14
- Compliance Measurement 14
- Exceptions 15
- Non-Compliance 15
12. Disclaimer 15
13. Consequence Management and Non-Compliance 15
14. Regulatory Compliance and Precedence 15
15. Policy Review 15

1. Introduction, Objective and Guiding Principles

1.1 Background

Mufin Green Finance Limited relies extensively on Information Technology ("IT") and digital channels for lending, collections, customer servicing, and internal operations. This dependence exposes the Company to cyber and technology risks that can affect the confidentiality, integrity, and availability of business and customer information, and consequently the Company's financial stability, regulatory standing, and reputation.

1.2 Objective

This Policy sets out the Company-wide framework for governance, identification, assessment, mitigation, monitoring, and reporting of Information Technology and Cybersecurity risk. Its objectives are to:

- Establish clear governance and accountability for IT and cybersecurity risk across the Board, Senior Management, and all functional departments;
- Prescribe baseline technical and procedural controls to protect information assets, customer data, and critical systems;
- Ensure the Company can anticipate, withstand, contain, and recover from cyber incidents with minimal disruption to business and customers;
- Ensure compliance with applicable RBI regulations, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025, and other applicable law;
- Embed a culture of cyber-risk awareness across every department of the Company.

1.3 Guiding Principles

- Confidentiality, Integrity and Availability (CIA) of information assets shall be preserved at all times, proportionate to the sensitivity and criticality of the asset.
- Security shall be built in by design across the technology and product lifecycle, not retrofitted.
- Access to information assets shall follow the principles of least privilege, need-to-know, and segregation of duties.
- Risk shall be managed on a risk-based, proportionate basis appropriate to the Company's scale, complexity, and NBFC-ML status.
- Every employee, contractor, and vendor personnel handling Company information is individually accountable for complying with this Policy.

2. Scope and Applicability

This Policy applies to:

- All employees, officers, directors, contractual staff, interns, and temporary personnel of the Company;
- All third parties, vendors, business correspondents, collection agencies, and service providers who access, process, store, or transmit the Company's information assets or customer data;
- All information assets owned, leased, or managed by the Company, including hardware, software, applications, networks, cloud environments, data (in any form or location), and facilities such as the Data Centre (DC) and Disaster Recovery (DR) site; and
- All Company departments, without exception, including: HR, Operations, Admin, Finance, InfoSec/IT, Legal, Lending/Business Function, Collections and Recovery, Customer Service and Complaints, and Credit.

This Policy shall be read together with the Company's Cybersecurity Policy, IT Governance Framework, Outsourcing Policy, Business Continuity and Disaster Recovery Policy, Data Protection and Privacy Policy, and IS Audit Policy, each of which shall be consistent with, and give effect to, the principles set out herein.

3. Definitions

Unless the context otherwise requires, the following terms shall bear the meanings assigned below (adapted from the FSB Cyber Lexicon and the AIFI Directions):

Term	Definition
Cyber Incident	A cyber event that adversely affects the cybersecurity of an information asset, whether resulting from malicious activity or not; includes both cybersecurity incidents and IT incidents.
Cyber Resilience	The Company's ability to continue carrying out its mission by anticipating and adapting to cyber threats and by withstanding, containing, and rapidly recovering from cyber incidents.
Cyber Threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.
Information Asset (IA)	Any piece of data, device, or component of the environment that supports information-related activities, including information systems, data, hardware, and software.
Privileged User	A user who, by virtue of function and/or role, has been allocated powers within an information system significantly greater than those available to the majority of users.
Recovery Time Objective (RTO)	The maximum tolerable length of time a system can be in the recovery phase before negatively impacting the Company's mission or business processes.
Recovery Point Objective (RPO)	The point in time to which data must be recovered after an outage.
Vulnerability	A weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.

4. Governance Structure and Roles

4.1 Board of Directors

The Board of Directors is the apex authority responsible for IT and cybersecurity governance and shall:

- Approve this Policy, the Cybersecurity Policy, and related frameworks, and review them at least annually;
- Ensure adequate budgetary allocation for IT and cybersecurity, commensurate with the Company's risk profile and threat landscape;
- Receive periodic (at least quarterly) briefings on the Company's cyber risk posture, incidents, and preparedness through the CISO and the Risk Management Committee of the Board / IT Strategy Committee.

4.2 IT Strategy Committee (ITSC)

The Company shall constitute a Board-level IT Strategy Committee comprising at least three directors, chaired by an independent director with substantial IT/cybersecurity expertise (minimum seven years' relevant experience). The ITSC shall meet at least quarterly and shall, inter alia:

- Guide and approve the Company's IT and cybersecurity strategy, ensuring alignment with business objectives;
- Oversee the IT Governance and Information Security Governance structures;

- Review budgetary allocation for IT and cybersecurity functions;
- Review, at least annually, the adequacy of Business Continuity Planning and Disaster Recovery arrangements;
- Approve documented standards for need-based access to information systems; and
- Review IT capacity assessments and remediation measures.

4.3 IT Steering Committee

An IT Steering Committee, comprising Senior Management representation from InfoSec/IT and business functions (Lending, Operations, Finance, Credit), shall meet at least quarterly to assist the ITSC in strategic IT planning, oversee BCP/DR processes, ensure a robust IT architecture, and update the ITSC and MD/CEO periodically.

4.4 Information Security Committee (ISC)

An Information Security Committee, headed by an officer from the Risk Management function and comprising the CISO and representatives from InfoSec/IT, Operations, Legal, Credit, and Business Function, shall operate under ITSC oversight and shall:

- Develop and implement information security / cybersecurity policies, standards and procedures;
- Approve and monitor cybersecurity projects and awareness initiatives;
- Review cyber incidents, IS audit observations, and mitigation activities; and
- Update the ITSC and MD/CEO periodically on ISC activities.

4.5 Chief Information Security Officer (CISO)

The Company shall designate a senior-level executive as CISO. The CISO shall not have a reporting relationship with the Head of IT Function and shall not be assigned business targets, in order to preserve independence. The CISO shall:

- Drive cybersecurity strategy and ensure compliance with regulatory instructions on information security/cybersecurity;
- Enforce information asset protection policies and coordinate cybersecurity issues internally and with external agencies (CERT-In, RBI, IDRBT, etc.);
- Be a permanent invitee to the ITSC and IT Steering Committee;
- Manage and monitor the Security Operations Centre and drive cybersecurity projects;
- Report directly to the Executive Director / Head of Risk Management function; and
- Place a review of cybersecurity risks, arrangements, and preparedness before the Board/RMCB/ITSC at least quarterly.

5. IT and Information Security Risk Management Framework

5.1 Periodic Review

The Company's enterprise-wide risk management policy shall incorporate IT and cybersecurity risk. The Risk Management Committee, in consultation with the ITSC, shall review and update this Policy and the associated risk register at least annually, or earlier upon a material change in the threat environment or business operations.

5.2 Framework Components

The IT and Information Security Risk Management Framework shall cover:

- Implementation of comprehensive information security controls and processes (including applicable cyber-insurance cover) to mitigate identified risks, reviewed periodically for efficacy;
- Clearly defined roles and responsibilities of stakeholders, including third-party personnel, with role conflicts and accountability gaps identified and eliminated or managed;
- Identification of critical information systems and fortification of their security environment; and
- Systems, procedures, and controls for secure storage, transmission, and processing of data.

5.3 Risk Identification, Assessment and Documentation

- Risk assessment of each information asset shall be guided by recognised security standards / IT control frameworks (e.g., ISO 27001, NIST CSF, COBIT).
- Inherent risk shall be assessed considering technologies adopted, business and regulatory alignment, organisational culture, and internal/external threats, and categorised as Low, Moderate, High, or Very High.
- Control evaluation shall factor in Board oversight, policies, cyber risk architecture, resourcing, training, threat intelligence arrangements, information-sharing arrangements (peers, RBI, CERT-In, IDRBT), preventive/detective/corrective controls, vendor management, and incident management.
- All staff and service providers shall comply with the Company's information security and acceptable-use policies.
- Security infrastructure and policies shall be reviewed at least annually, factoring in emerging threats including phishing and spoofing attacks.

6. Baseline Cybersecurity and Resilience Requirements

The InfoSec/IT Department, in coordination with Operations, Admin, Finance, Legal, and the business functions identified against each control area, shall implement and maintain the following baseline controls.

A. Inventory Management of Information Assets

- Maintain an up-to-date inventory of information assets (data, applications, infrastructure, key personnel, facilities) indicating business criticality — owned by InfoSec/IT.
- Classify data/information based on sensitivity criteria (Public, Internal, Confidential, Restricted).
- Maintain an enterprise data dictionary to promote common understanding of data across applications.
- Manage and protect data within and outside Company network borders proportionate to sensitivity and risk.

B. Data Leak Prevention (DLP)

- Develop and operate a data loss/leakage prevention strategy covering endpoint, in-transit, and at-rest data, including at vendor-managed facilities.
- Preserve confidentiality, integrity and availability of customer personal and sensitive data across its lifecycle, including with third-party vendors.
- Implement remote wipe/lock/management controls for mobile devices and laptops.

C. Data Migration Controls

- Maintain a documented data migration policy ensuring data integrity, completeness and consistency, with audit trails and business/application-owner signoffs at each migration stage.

D. Preventing Execution of Unauthorised Software

- Maintain a centralised inventory of authorised/unauthorised software; consider application/library whitelisting.
- Control installation of software centrally on PCs, laptops, servers, mobile devices and cloud environments; block unauthorised installation.
- Monitor vendor/OEM/CERT-In patch advisories and deploy security patches expeditiously, with an emergency patch process for actively exploited critical vulnerabilities.
- Maintain a documented exception policy specifying justification, duration, approval authority, and periodic review of granted exceptions.

E. Physical and Environmental Controls

- Secure the Data Centre (DC) and Disaster Recovery (DR) site from natural and man-made threats.

- Monitor breaches of environmental controls (temperature, water, smoke, power, telecom, access alarms and logs) — Admin Department to coordinate physical security with InfoSec/IT.
- Ensure DC and DR sites are geographically well separated and subject to e-surveillance.

F. Capacity Management

- Ensure information systems support business functions and availability of all service delivery channels.
- Assess IT capacity requirements at least annually, consistent with peak usage trends, current needs and projected growth.

G. Secure Configuration

- Document and apply baseline security configurations across endpoints, mobile devices, operating systems, databases, applications and network/security devices, throughout their lifecycle, with periodic review.
- Periodically evaluate critical devices (firewalls, switches, security devices) including configuration and patch levels across the Company's network, DC, and any third-party hosted sites.

H. Network Management and Security

- Permit only authorised, time-bound, audited network access, with responsibility resting with Company officials.
- Maintain an up-to-date network architecture diagram (wired/wireless) and a centralised inventory of authorised connected devices.
- Secure wireless LANs, access points and client access systems; automatically identify and block unauthorised device connections.
- Maintain multi-layered boundary defences (firewalls, proxies, DMZ, IPS/IDS) with real-time inbound/outbound traffic filtering.

I. Application Security Lifecycle

- Embed information security across all stages of the application lifecycle, including secure coding practices for internally/collaboratively developed applications.
- Specify security requirements (access control, authentication, transaction authorisation, audit trail, session management) during development/acquisition.
- Segregate development, test, and production environments.
- Conduct security testing aligned with OWASP and other recognised standards, adopting defence-in-depth; testing shall not be limited to the OWASP Top 10.
- Periodically test web/mobile applications pre-implementation, post-implementation and after changes, in a production-like environment.
- Obtain vendor certification/confirmation that applications are free of known vulnerabilities, malware and covert channels, including on material changes.

J. Maintenance, Monitoring and Analysis of Audit Logs

- Ensure every IT application/system handling critical or sensitive information has audit logging capability and produces audit trails (date, timestamp, source/destination address, event details).
- Regularly monitor audit trails and system logs to detect, understand or recover from unauthorised activity.

K. Patch, Vulnerability and Change Management

- Maintain documented change and patch management policy assessing business impact, applying approvals, and enabling rollback from failed changes.
- Adopt a documented, risk-based strategy for inventorying, identifying and timely patching of vulnerable IT components, including end-user devices, servers, databases, and middleware.
- Determine root cause of detected incidents and implement corrective patches.

L. User Access Control / Management

- Grant access to information assets only on valid business need (need-to-know, least privilege).
- Closely supervise and log activity of personnel with elevated/privileged access, with periodic review.
- Protect data at rest (encryption) and in transit (VPN/secure protocols); protect access credentials against leakage.
- Disallow administrative rights on end-user devices by default; grant on need-to-know basis for defined duration.
- Implement centralised authentication/authorisation, strong password policy, and mandatory multi-factor authentication for privileged users of critical systems and critical activities.
- Minimise invalid logon attempts, deactivate dormant accounts, and monitor abnormal logon patterns.

M. Controls on Teleworking / Work-from-Home

- Ensure secure remote access from alternate work locations to Company systems, with multi-factor authentication for critical systems.
- Identify all remote-access devices connected to Company systems and ensure data shared during teleworking is appropriately secured.

N. Authentication Framework for Customers

- Implement positive identity verification for customers across all delivery channels (web, mobile app, physical branch/partner touchpoints) and enable customers to verify the Company's authenticity.

O. Secure Mail and Messaging Systems

- Implement anti-spoofing, look-alike domain protection, malicious attachment/link protection, and spam filtering; require similar measures from vendors and partners.
- Implement DMARC for Company email domains and control permissible attachment types.

P. Removable Media

- Disallow removable devices/media by default unless specifically authorised for defined use and duration.
- Scan removable media for malware before granting access; limit data types transferable to/from such devices.

Q. Third-Party / Vendor Arrangements

- Conduct a documented vendor risk assessment proportionate to risk and materiality, addressing concentration risk, conflicts of interest, single points of failure, data protection compliance, availability, and supply chain risk — coordinated jointly by InfoSec/IT and the relevant business owner (e.g., Collections and Recovery for recovery agencies, Lending/Business Function for DSAs/BC partners).
- Conduct due diligence, oversight and ongoing management of vendors/service providers, with contractual audit rights for the Company and for RBI/persons authorised by RBI.
- Ensure background checks, non-disclosure agreements, and security policy compliance agreements for all third-party personnel accessing Company assets — coordinated by HR and Legal for onboarding-linked personnel.

R. Cryptographic Controls

- Use strong, internationally accepted, non-deprecated key lengths, algorithms, cipher suites and protocols for data in transit, at rest, and for authentication, compliant with extant law.

S. Straight Through Processing (STP)

- Prevent unauthorised manual modification of data transferred between processes/applications for critical applications; ensure such transfers are tested, automated, and audit-trailed.

T. Continuous Surveillance / Cyber Security Operations Centre (CSOC)

- Operate a CSOC (in-house or through a managed security service provider) to ensure continuous surveillance and stay updated on emerging threats — see Section 7.

U. Advanced Real-Time Threat Defence and Management

- Build defence against installation, spread and execution of malicious code across endpoints, servers, gateways, wireless networks, and SMS/OTP delivery systems, with centralised management and monitoring.
- Implement whitelisting of internet websites/systems and consider secure web gateways with deep packet/HTTPS inspection.

V. Anti-Phishing

- Subscribe to anti-phishing / anti-rogue-application services for identifying and taking down phishing sites/applications impersonating the Company.

W. Vulnerability Assessment and Penetration Testing (VA/PT)

- Conduct periodic VA/PT for all critical and internet-facing systems, applications, servers and network components, across pre-implementation, post-implementation and post-change stages.
- For critical/customer-facing DMZ systems: VA at least every six months, PT at least annually; risk-based periodicity for non-critical systems.
- Use independent, appropriately credentialed (preferably CERT-In empanelled) auditors; review scope, coverage and auditor performance on an ongoing basis.
- Remediate identified vulnerabilities in a time-bound manner and report closure status to the ISC/ITSC at least quarterly.

X. Red Teaming Exercises

- Consider periodic red teaming exercises simulating real-world adversarial attacks to test defences and mitigating controls.

Y. Business Continuity Planning (BCP) and Disaster Recovery (DR)

- Adopt a BCP/DR policy based on recognised standards (e.g., ISO 22301), reviewed on major developments and risk assessments.
- Conduct DR drills for critical systems at least half-yearly, covering a full business day (Beginning of Day to End of Day) at the DR site; resolve and retest major issues before the next cycle.
- Periodically back up data and test restoration; maintain identical configuration/patch levels at DC and DR; prioritise minimal RTO and near-zero RPO for critical systems, with a documented reconciliation methodology where RPO is non-zero.
- Extend BCP/DR readiness expectations to critical interconnected vendor and partner systems through coordinated resilience testing.

Z. Cyber Incident Response and Recovery Management

- Maintain a documented Cyber Incident Response and Recovery Management Policy covering incident classification, roles/responsibilities, reporting channels (employees, vendors, customers), communication strategy, containment/recovery measures, threat-information sharing, post-incident review, and periodic testing of response plans.
- Provide specialised training to personnel handling cyber incidents and incorporate lessons learnt to continually improve response plans.

- Document strategies for advanced attacks (ransomware/cyber extortion, data destruction, DDoS) and contain attacks via shielding/quarantine of affected systems.
- Analyse incidents (including forensic analysis where necessary) for severity, impact and root cause, and take corrective/preventive measures.
- Report cyber incidents to the Board/Senior Management per escalation protocol; report to RBI and proactively notify CERT-In within regulatory timelines applicable to the Company as an NBFC.
- Maintain a Cyber Crisis Management Plan (CCMP), forming part of the Board-approved cybersecurity framework, addressing Detection, Containment, Response and Recovery for threats including DDoS, ransomware, destructive malware, business email fraud, phishing (including spear-phishing and whaling), vishing, and identity/credential fraud.

AA. Metrics

- Develop key performance and key risk indicators (anti-malware coverage/updation, patch latency, awareness training coverage, vulnerability metrics, RTO/RPO adherence) and report periodically to the ISC/ITSC.

BB. User / Employee / Management Awareness

- Define and communicate security policies to all users, vendors and partners, with mandatory induction training for all new recruits (coordinated by HR and InfoSec/IT) and annual refresher training for all staff, including lower/middle management.
- Provide targeted training for executive, operational and security-administration personnel, and annual Board/Senior Management sensitisation on evolving cyber threats.
- Encourage and enable reporting of suspicious behaviour/incidents to the incident management team; evaluate employee awareness levels periodically.

CC. Customer Education and Awareness

- Maintain ongoing customer awareness programmes on cybersecurity risks, coordinated by Customer Service and Complaints Team with InfoSec/IT.
- Encourage customer reporting of phishing mail/sites, with effective remedial action on reporting; educate customers on risks of sharing login credentials, passwords, OTPs and PINs.

DD. Risk-Based Transaction Monitoring

- Implement risk-based transaction monitoring/surveillance as part of the fraud risk management system across all delivery channels, jointly owned by Operations, Finance, and Collections and Recovery, with InfoSec/IT providing tooling support.

EE. Forensics

- Maintain arrangements (in-house or on standby with external specialists) for network forensics, forensic investigation, and DDoS mitigation services.

7. Cyber Security Operations Centre (CSOC)

7.1 Governance

The Company shall establish and operate a CSOC (which may be an in-house facility or a managed detection and response service, given the Company's scale as an NBFC-ML), commensurate with its technology risk profile, scale, and regulatory obligations. Governance arrangements shall include periodic briefing of the ITSC/Board on threat intelligence, oversight dashboards, a defined reporting policy, and timely stakeholder communication.

7.2 Capabilities

- Proactive monitoring using SIEM tooling: log collection, correlation, dashboard-based anomaly detection, and alert/incident escalation.

- Root-cause identification, attack classification, incident investigation, dynamic behaviour analysis, IOC collection, geo-location analytics, and (where appropriate) honeypot services.
- Responsibility for monitoring, analysing and escalating security incidents; executing response measures across protect-detect-respond-recover phases; incident management and forensic analysis; and coordination with internal contact groups and external agencies (CERT-In, RBI, IDRBT).

7.3 Staff Capabilities

- Level 1 — round-the-clock monitoring by trained personnel with relevant certifications (may be outsourced to a managed CSOC provider under a documented SLA).
- Level 2 — specialised network, data and endpoint security expertise for root-cause analysis and corrective action.
- Level 3 — advanced SOC analyst capability for deep packet analysis, IOC collection, forensic evidence handling and malware analysis, sourced in-house or via a competent managed service provider, with clear accountability retained by the CISO's office regardless of sourcing model.

8. Information Systems (IS) Audit

- The Audit Committee of the Board (ACB) shall exercise oversight of IS Audit.
- The Company shall maintain a Board-approved IS Audit Policy describing mandate, purpose, authority, audit universe and periodicity, reviewed at least annually.
- IS Audit shall be conducted by a separate IS Audit function/resource with requisite skills, within or reporting into Internal Audit; where external resources are used, accountability remains with Internal Audit.
- IS Audit planning shall follow a risk-based approach, with continuous auditing considered for critical systems.
- The ACB shall review critical IT/InfoSec/cybersecurity issues raised in audits and direct Management accordingly.

9. Departmental Roles and Responsibilities

While the CISO and the InfoSec/IT Department own this Policy and the technical control environment, information and cyber security is a shared responsibility across the Company. The table below summarises department-level accountability.

Department	Key Information & Cyber Security Responsibilities
HR Department	Background verification of new hires and contractual staff; mandatory information security induction training and annual refresher training; enforcement of acceptable-use undertakings and confidentiality agreements; prompt off-boarding (access revocation) coordination with InfoSec/IT on exit; reporting of policy violations linked to personnel conduct.
Operations	Adherence to secure operating procedures for transaction processing, STP controls, and segregation of duties; reporting of unusual system/process activity; participation in BCP/DR drills; risk-based transaction monitoring support.
Admin	Physical and environmental security of offices, DC/DR premises and access-controlled areas; visitor management; asset tagging and physical asset inventory support; coordination with InfoSec/IT on CCTV/e-surveillance and environmental monitoring.
Finance	Budgetary allocation for IT/cybersecurity in line with ITSC guidance; financial controls over vendor payments tied to verified deliverables;

Department	Key Information & Cyber Security Responsibilities
	support for cyber-insurance evaluation; fraud-loss and incident cost reporting; risk-based transaction monitoring for financial irregularities.
InfoSec / IT	Policy ownership, control design and implementation, CSOC operations, patch/vulnerability/change management, access management, VA/PT coordination, incident response execution, BCP/DR technical readiness, and all baseline controls in Section 6, under CISO/Head of IT Function leadership.
Legal	Review and vetting of vendor/outsourcing contracts for security, audit-rights and data-protection clauses; regulatory liaison support for incident reporting obligations (RBI, CERT-In, DPDP Act); advising on data breach notification obligations; IP and confidentiality protections.
Lending / Business Function	Secure handling of applicant/customer data during origination; adherence to customer authentication framework across lending channels; oversight of DSA/BC partner compliance with data-handling requirements; escalation of suspected application fraud.
Collections and Recovery	Secure handling of customer contact and repayment data; oversight of third-party collection agency compliance with data protection and acceptable-use requirements; reporting of data-handling incidents involving field/recovery agents.
Customer Service and Complaints Team	Customer authentication verification during service interactions; customer education and awareness on phishing/OTP/credential-sharing risks; first-point capture and escalation of customer-reported security incidents and phishing complaints to InfoSec/IT.
Credit Team	Secure handling of credit bureau data and applicant financial information; access control adherence on credit decisioning systems; reporting of anomalies suggestive of data manipulation or identity fraud.

10. Exceptions, Non-Compliance and Policy Enforcement

- Any exception to this Policy shall be documented with business/technical justification, defined duration, and approved by an officer at a senior level equipped to evaluate the risk, with periodic review of all granted exceptions.
- Non-compliance by an employee may result in disciplinary action up to and including termination, in accordance with the Company's HR policies; non-compliance by a vendor/service provider shall be dealt with per the relevant contractual terms, up to termination of the arrangement.
- All confirmed cyber incidents and material policy violations shall be reported to the ISC and, where applicable, to the Board/ITSC, RBI and CERT-In within applicable regulatory timelines.

11. 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 (***Refer - MGFL/EMP/POL/00***) 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.

12. 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.

13. 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.

14. 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.

15. 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.

****