SATYA MICROCAPITAL LIMITED

Information System Audit Policy

Version 2.0

Document review and approval

Name of the document	Information System Audit Policy
Approving Authority	Board of Directors
Date of Approval	May 29, 2026
Effective date of the Policy	Board Approval date
Policy Owner	IT Department
Finalized/Reviewed by	Ashutosh Kumar Srivastava, Chief Technology Officer
Review Frequency	Annually and upon need basis
Version No.	2.0

Version Control

Sr. No.	Version No.	Revision remarks	Effective Date	Approved by
1.	1.0	First Approval	13/11/2021	Board of Directors
2.	1.1	Align with the suggestions made by the investors	10/05/2025	Board of Directors
3.	2.0	Align with regulatory requirement	29/05/2026	Board of Directors

Table of Contents

1. INTRODUCTION

SATYA MicroCapital Limited is a Public Limited Company incorporated under the provisions of the Companies Act, 1956 and validly existing under the provisions of the Companies Act, 2013, having Corporate Identification Number (CIN) U74899DL1995PLC068688 (hereinafter referred to as "SATYA" or the "Company"). SATYA is a Middle Layer Non-Deposit taking Non-Banking Financial Company ("NBFC"") registered and regulated by the Reserve Bank of India ("RBI") as a Non-Banking Financial Company – Micro Finance Institution ("NBFC - MFI"), bearing Registration no. 14.01513.

The Company is engaged in the business of providing Microfinance Loans to borrowers from low-income households, primarily in rural and semi-urban areas, which include Water & Sanitation loans, Micro, Small and Medium Enterprises Business loans, Limited liability loans, etc. The Company primarily focuses on empowering rural women both digitally and financially and facilitate financial inclusion.

2. PURPOSE OF INFORMATION SYSTEM AUDIT

In the digital age, a company's information systems serve as the backbone of its operations, enabling seamless functionality, decision-making, and strategic advancements. As these systems grow in complexity and significance, ensuring their security, reliability, and compliance becomes paramount. Recognizing the critical role these systems play, the Company is committed to routinely auditing its information infrastructure. The objective of the IS Audit is to provide an insight into the effectiveness of controls that are in place to ensure confidentiality, integrity, and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc. By adhering to this policy, we aim to bolster our defense against potential cyber threats, uphold our regulatory commitments, and safeguard our company's reputation, data, and digital assets. It serves as a roadmap for both internal teams and external stakeholders, underscoring our unwavering commitment to information, integrity and security.

3. REGULATORY REFERENCE

This policy has been framed in accordance with the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, as amended from time to time, (hereinafter, RBI ITGRC Directions). In case of any conflict or ambiguity, the guidance mentioned under RBI ITGRC Directions shall be followed with.

4. DEFINITIONS

'Information System' - Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks.

'Cyber security' Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

5. SCOPE OF IS AUDIT

IS Audit shall cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit shall also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that Business Continuity Plan (BCP) is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance with all the applicable legal and statutory requirements.

The IS audit universe or scope encompasses all of the Company's information systems, encompassing Core Business Applications, databases, servers, network infrastructure, cloud services, and associated IT equipment and processes. The policy is applicable to all departments, units, and operations of the company where

information systems are employed, irrespective of their geographical location or functional domain. This includes systems managed in-house as well as those outsourced to third-party vendors or hosted on external platforms. All employees, contractors, consultants, and any other individuals or entities accessing or managing the Company's IT resources are expected to comply with this policy. Additionally, the policy integrates considerations from regulatory mandates, industry standards, and best practices to ensure comprehensive coverage and robust scrutiny of our information system environment.

6. ROLE AND RESPONSIBILITIES

The following section outlines these roles and responsibilities, serving as a guidepost for all involved in this information system audit process.

Board of Directors

- Retain ultimate ownership of the Information System Audit Policy.
- Approve, periodically review, and amend the policy as required.
- Ensure that the policy's objectives align with the company's strategic goals and that its implementation is monitored and enforced.

Audit Committee of the Board (ACB)

The Audit Committee of the Board (ACB) is an integral facet of the Company's governance structure, the ACB shall be responsible for ensuring that the policy's stipulations are not only adhered to but also remain congruent with the Company's overarching objectives and the prevailing regulatory landscape. The committee shall review the audit's scope, objectives, findings, and recommendations, ensuring that they align with the Company's strategic goals and that potential risks are addressed proactively. Additionally, the ACB shall liaise with the internal audit team, external auditors, and relevant stakeholders, fortifying the lines of communication and fostering a collaborative environment conducive to thorough and effective auditing.

Furthermore, the ACB shall serve as the primary point of escalation for any significant discrepancies, challenges, or concerns identified during the audit. In scenarios where critical vulnerabilities are unearthed or where there's a divergence between the audit team's recommendations and management's perspective, the ACB shall intervene to arbitrate and guide the decision-making process. The ACB shall review critical issues highlighted related to IT / information security / cyber security and provide appropriate direction and guidance to the management of the Company. By taking on this pivotal role, the Audit Committee of the Board ensures that the Information System Audit Policy is not just a procedural mandate but a living, evolving framework that continually enhances the organization's security posture, compliance, and operational resilience.

Head of Internal Audit

The Head of Internal Audit is responsible for developing, implementing, and maintaining the IS audit function in accordance with this policy. The Head of Internal Audit shall report to the ACB on the effectiveness of the IS audit program and any significant findings or recommendations.

Internal Audit Team

The Company shall formulate a separate IS audit function with resources who possess required professional skills and competence within the Internal Audit function. The following roles shall be performed by such function:

- Conduct regular audits as defined by the policy.
- Document findings, prepare audit reports, and present them to the Board and other relevant stakeholders.
- Propose corrective actions based on audit findings.

IT Team and DevOps Team & Software Development team:

- Adhere to the policy and cooperate during audits.
- Provide technical assistance and access to systems, logs, and data during the audit process.
- Implement corrective actions as directed by the Internal Audit Team based on audit findings.

External Auditors (when engaged):

- Provide an impartial evaluation of the information systems, drawing upon industry standards and best practices.

- Offer specialized knowledge and insights that may not be available in-house.
- Share findings, risks, and recommendations with the ACB or the Board.

All Employees and Contractors:
- Comply with the policy and cooperate during the audit process.
- Provide necessary information or access when required during the audit.
- Stay informed about the policy's updates and participate in any training or awareness programs.

7. INFORMATION SYSTEM AUDIT PROCESS

The information System Audit Process has defined the comprehensive approach to fulfill the needs of the organisation. The details of audit approach are as follows:

Approach
The purpose of audit approach is to enable the development of a strategic work plan that is designed to best meet the organizations objectives. The approach in summary entails the following key phases:

The audit approach has 5 steps to laying down the strong internal audit foundation. The details of the above- mentioned graph are as follows:

Audit Plan Development –

The audit plan is designed to identify and concentrate on areas of importance, to provide an effective and efficient review and seek to add value to the organization's activities. Detailed plans are prepared and updated annually. In the audit planning it is important to identify the key auditable areas followed by the plan approval and plan review and update.

The Company shall follow a risk-based audit approach for IS Audit planning. To plan and execute the IS audit, the following steps shall be involved:

- Planning the audit to gain a sufficient understanding of the targeted area of coverage and related aspects.
- Business/process objectives to define the scope, timing, and resource requirements of the audit.
- Creating a work plan detailing each step of audit, its timing, and the date of closure.
- Intimation to the departments being audited about the start and tentative closure date for the internal audit.
- Engaging stakeholders to discuss the audit approach, processes to be covered, applicable risks, etc.
- Walk-throughs with the relevant process owner shall be performed and documented by the auditors.
- Documenting a Risk and Control Matrix (RCM) to perform an evaluation of overall control design effectiveness in terms of mitigating significant risks inherent in the scoped processes and confirm control design findings/gaps and understanding with the business departments.
- Controls are tested to determine if they have operated as designed throughout the period under review.
- Rating the issues/ observations into Critical, High, Moderate, Low and Process Improvement.
- Communicate the observations to the Audit Committee after discussion with the department heads and other key stakeholders and document an action plan in the report.
- Monitoring and follow-up of the action plan on the issues.

In performing our Statutory Audit of Financial Statement in accordance with the applicable Standards and laws, we intend to obtain a reasonable assurance on the automated/programmed controls. Our reliance on automated programmed controls depends on effectiveness of IT General Controls. Accordingly, we need to perform a review

of IT General Controls.

Therefore, in SATYA following areas have been identified and priorities which shall be audited by the third party on a quarterly basis.

1. Program Development/Change involving
   - Test
   - Version Control
2. Logical Access Controls for the identified applications involving
   - Granting
   - Modification
   - Deletion
   - Password Controls
   - Critical id management
   - Remote Access Management
   - Access Controls over Version Control software (if Version Control software is used)
3. Security Management Process involving
   - Hardening of OS and Database
   - Infrastructure Change management
4. Computer Operations
   - Backup of data and applications
   - Job scheduling / monitoring of interfaces
   - Incident / problem management
5. Application Controls
6. Business Continuity and Disaster Recovery
7. Cloud Security
8. Compliance with Regulatory Standards
9. Incident Response Plan
10. User Training and Awareness
11. Physical Security
12. Vendor Management
13. Patch Management
14. Log Management and Monitoring
15. End-Point Security

Audit Programme Delivery

Specific audits will be undertaken in accordance with the agreed audit plan. The key steps and audit approach in conducting an audit are highlighted below:

Key Stages	→	Approach
Research Planning and information gathering	→	Define the objectives Review documentation and policies and procedures Interviews with relevant key stakeholders or undertake file work
Evaluation and Analysis	→	Evaluation and Analysis based on the collected information
Reporting and Strategy Development	→	Draft Report Issue Final Audit Report

Audit Reporting and Documentation

The third-party Audit team will report to SATYA's management which includes MD, Dy CEO, CRO and IT Head on a quarterly basis on:

- Audits completed
- Progress in implementing Internal Audit work plans
- The status of implementation of agreed audit recommendations.

Once the audit findings are reviewed by the management. The audit findings are further reported to the IT Strategy Committee.

Further, the company may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.

IS Audit observations shall also be reviewed by Information Security Committee (ISC) of the Company.

Active user review by Internal Auditor

The Internal Auditor shall perform quarterly reviews of active users on BR.net against HR records to ensure no unauthorized users exist in the system. This process involves verifying the alignment of user access with current employee status and roles, identifying any discrepancies, and taking corrective actions as necessary. The findings from these reviews shall be documented and reported to the IT Strategy Committee for oversight and further action.

8. IT STRATEGY COMMITTEE

IT Strategy Committee is set up to effective implementation of Cyber Security Policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. The Committee shall meet at least on quarterly basis. The committee shall comprise of

i. Minimum of three directors as members

ii. The Chairperson of the ITSC shall be an independent director and have substantial IT expertise in managing/ guiding information technology initiatives; and

iii. Members are technically competent

CISO shall be the permanent invitee

Following are the Roles and Responsibilities of IT Strategy Committee:

- Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.
- Ascertaining that management has implemented processes and practices that ensure that IT delivers value to the business.
- Ensuring IT investments represent a balance of risks and benefits, and those budgets are acceptable.
- Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.
- Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.
- Ensuring that Committee should meet atleast on quarterly intervals.
- all other roles and responsibilities as prescribed under RBI ITGRC Directions.

9. COMPLIANCE

SATYA management and IT Department are responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Also, Internal Audit's performance encompasses the following responsibilities:

- To ensure all work complies with internationally recognized standards;
- To maximize use of resources;
- To minimize costs;
- To supplement resources where necessary with professional expertise on an as required basis.

The company is committed to ensuring adherence to the requirements outlined in the RBI ITGRC Directions.

10. POLICY REVIEW

Annual review of this policy shall be done by the ACB as well as the Board of Directors of the Company.

11. OMNIBUS CLAUSE

All extant & future master circular/directions/guidance/guidance notes issued by RBI from time to time would be the directing force and will super cede the contents of this policy.