CHANGE MANAGEMEMENT POLICY

Industrial Investment Trust Limited
CIN: L65990MH1933PLC001998
Regd. Off: 101A, The Capital, G-Block,
Plot no.C-70 Bandra Kurla Complex,
Bandra (East) Mumbai Mumbai City
MH 400051
Website: www.iitlgroup.com

Version	Date of Approval/ Reviewal
V.2	23-05-2026
Recommended By	CEO NBFC
Approved By	Board Meeting Dated – 23-05-2026

CHANGE MANAGEMEMENT POLICY

1. Introduction

1.1 Purpose of the Policy

This policy has been meticulously crafted in strict adherence to the directives delineated within the Reserve Bank of India (RBI) master direction RBI/DNBS/2016-17/53, specifically under Master Direction DNBS.PPD.No.04/66.15.001/2016-17. The paramount objective of this Change Management Policy is to institute a comprehensive framework ensuring that all modifications to both the Information Technology (IT) infrastructure and business operations within the organization are meticulously executed in a manner that adheres rigorously to legal and regulatory protocols as stated in the master direction RBI/DNBS/2016-17/53, specifically under Master Direction DNBS.PPD.No.04/66.15.001/2016-17 . The central tenet of this policy is to mitigate the potential adverse repercussions of change-related incidents on service quality and delivery, streamline business processes, and unequivocally uphold adherence to the statutory and regulatory stipulations promulgated by the Reserve Bank of India governing the financial sector.

1.2 Scope and Applicability

This policy is hereby declared to be applicable to any and all modifications, alterations, or amendments in technology, business processes, and operational procedures undertaken within the organization. Encompassed within its purview are adjustments to both software and hardware components, modifications to network configurations, updates to applications, and any other alterations that may have an impact on the Information Technology (IT) infrastructure or business operations. Furthermore, this policy shall ensure the establishment of meticulous audit trails and the implementation of Standard Operating Procedures (SOPs) to facilitate the execution of proposed changes.

It is expressly stipulated that this policy is binding upon all employees, contractors, and third-party service providers involved in the change management process, and compliance with its provisions is mandatory.

1.3 Definitions and Key Terms

1.3.1 Change refers to any intentional modification within a business's IT infrastructure or operations that could impact services or processes. This includes alterations like updates, installations, and configurations, whether initiated internally or externally. Changes must

adhere to laws, regulations, and internal policies, with considerations for factors such as risk, compliance, and stakeholder interests. Formal change management processes are implemented to classify, prioritize, and manage changes, ensuring adherence to standards and mitigating risks. Unauthorized changes are strictly prohibited, with disciplinary actions or legal remedies enforced for non-compliance. Designated individuals or entities oversee the change management process to maintain effectiveness, efficiency, and integrity.

1.3.2 Change Management : Change Management is the structured process through which organizations manage alterations to their systems, processes, and resources. It involves identifying the need for change, submitting formal requests, assessing proposed changes for feasibility and impact, and obtaining approval from designated authorities. Once approved, changes are implemented systematically with detailed plans and coordination to minimize disruption and ensure compliance. Following implementation, changes are reviewed and evaluated to measure outcomes and gather feedback for continuous improvement. Effective communication, stakeholder engagement, and governance mechanisms are vital throughout the process to foster transparency and organizational adaptability. Formal frameworks and a commitment to continuous improvement drive success in Change Management..

1.3.3 Change Advisory Board (CAB): The Change Advisory Board (CAB) is a structured and multidisciplinary group within an organization tasked with the critical responsibility of evaluating, scrutinizing, and authorizing significant changes to the organization's systems, processes, technologies, policies, or infrastructure before their implementation. Comprising key stakeholders, subject matter experts, and decision-makers from various departments or functional areas, the CAB serves as a central governance body that ensures thorough consideration, informed decision-making, and risk management throughout the change management lifecycle. The CAB's primary objective is to uphold the stability, integrity, and reliability of the organization's operations by assessing proposed changes in terms of their potential impact, feasibility, alignment with strategic objectives, and adherence to regulatory requirements, industry standards, and best practices.

1.3.4 Impact Assessment: Impact Assessment is a methodical and comprehensive process utilized by organizations to thoroughly analyze and evaluate the potential effects, consequences, and implications of a proposed change on various facets of the organization's operations, services, and stakeholders. It encompasses a series of structured activities aimed at understanding the scope, magnitude, and nature of the impacts that the proposed change may have, enabling informed decision-making, risk management, and resource allocation throughout the change management lifecycle.

1.3.5 Rollback: The process of reverting changes to a previous state if the implementation fails or causes unexpected issues.

1.3.5 Documentation :- Documentation prepared to support proposed change, implementation, approvals and with rollback statement, if any.

2. Regulatory Framework

2.1 Overview of RBI's Master Direction relevant to IITLs

This has reference to RBI Circular No. RBI/DNBS/2016-17/53 Master Direction; DNBS.PPD.No.04/66.15.001/2016-17 dated 08th June, 2017, wherein the Reserve Bank of India (RBI) had prescribed to govern the operational and regulatory framework of Non Banking Financial Companies (IITLs) in India. These directions cover various aspects such as capital requirements, governance standards, reporting mechanisms, and specific operational guidelines, including the management of IT resources and cybersecurity.

2.2 Legal and Compliance Obligations

IITL to comply with the RBI's regulations, ensuring financial stability, transparency, and integrity in our operations. This includes adherence to guidelines on capital adequacy, risk management, KYC norms, anti-money laundering standards, and consumer protection, and any other directions , various notifications, circulars issued by the RBI on time to time. Compliance with these regulations is critical to maintain licensure and avoid legal penalties.

2.3 Alignment with Industry Best Practices

In addition to adhering to the regulatory guidelines set forth by the Reserve Bank of India (RBI), our organization is committed to aligning our operational practices with globally recognized and locally relevant industry best practices for financial institutions.

This strategic alignment encompasses the adoption of comprehensive frameworks such as those for information security and IT service management, which are widely acknowledged as benchmarks for excellence in the financial sector.

2.4 Documentation :-

As an entity registered with the Reserve Bank of India (RBI), it is incumbent upon IITL to ensure the meticulous documentation of all proposed changes and their impacts, while also maintaining proper audit trails to uphold transparency.

3. Change Management Process

3.1 Prioritizing and responding to change proposals from business:

Evaluation and response to business change proposals involve assessing their impact on organizational objectives, strategic alignment, and resource availability. Prioritization is based on urgency, ROI, and alignment with corporate goals & Compliance perspective. Understanding the need of the Change request is very important.

3.2. Cost-benefit analysis of the changes proposed:

Conducting a cost-benefit analysis is essential to determine the financial feasibility and potential value of proposed changes. This involves quantifying both direct and indirect costs associated with implementation, alongside estimating expected benefits such as revenue growth, cost savings, Compliance or competitive advantage. Decision-making is guided by comparing costs against anticipated benefits.

3.3. Assessing risks associated with the changes proposed:

Thorough risk assessment is vital to identify potential obstacles, uncertainties, and negative impacts related to proposed changes. Factors such as complexity, stakeholder resistance, and

external dependencies are considered. Strategies are developed to mitigate risks and enhance the likelihood of successful implementation.

3.4. Change implementation, monitoring, and reporting:
Effective implementation, monitoring, and reporting mechanisms are crucial for successful change execution. This entails executing planned activities, allocating resources, and managing transitions while minimizing operational disruptions. Monitoring progress involves tracking key performance indicators and milestones, while reporting ensures transparency and accountability to stakeholders through regular updates and performance reviews.

4. Roles and Responsibilities

4.1 Change Advisory Board (CAB)
The CAB evaluates significant change proposals, ensuring they align with strategic goals and assessing potential impacts. It comprises members from various departments, providing diverse perspectives.

4.2 Change Manager/Coordinator
This role oversees the change management process, from initiation to post implementation review. Responsibilities include ensuring adherence to the policy, coordinating between teams, and managing documentation.

IITL to identify a designated manager who to be responsible for initiation of the change and its implementation.

There to be a person responsible for the monitoring of the change and review the implementation of the change.

4.3 IT Department and Other Operational Teams
These teams implement changes, ensuring technical compatibility and operational continuity. They also provide feedback on the feasibility and potential challenges of proposed changes.

4.4 External Stakeholders
When changes affect external partners or customers, our input and concerns are addressed. This ensures smooth transitions and maintains positive relationships.

5. Risk Management

5.1 Risk Identification and Categorization
This phase involves systematically identifying potential risks associated with proposed changes, including technical, operational, financial, and compliance risks. Each identified risk is categorized based on its nature and potential impact on the organization.

5.2 Mitigation Strategies and Contingency Planning

For each identified risk, mitigation strategies are developed to minimize or eliminate the risk's impact. Contingency plans are also established for critical risks, outlining steps to be taken if the risk materializes.

1. Risk Analysis and Prioritization: Each identified risk to be analysed for its potential impact and likelihood and prioritized accordingly.

2. Development of Mitigation Strategies: For each prioritized risk, tailored mitigation strategies to be formulated to either reduce the likelihood of the risk occurring or to lessen its impact should it occur.

3. Establishment of Contingency Plans: For risks deemed critical, contingency plans to be developed. These plans to detail actionable steps and allocate resources to ensure rapid response capabilities.

4. Assignment of Responsibilities: Clear responsibilities to be assigned for the implementation of mitigation strategies and the activation of contingency plans.

5. Regular Monitoring and Review: The effectiveness of mitigation strategies and the readiness of contingency plans to be regularly monitored and reviewed, with adjustments made as necessary to address evolving risk landscapes.

5.3 Periodic Review and Reporting of Risk Status
Regular reviews of the risk landscape and the effectiveness of mitigation measures are essential. Reporting mechanisms should be in place to update stakeholders on the status of risks and the outcomes of mitigation efforts.

6. Change Implementation
This involves creating a comprehensive plan that outlines the steps, timelines, and resources required for implementing the change. Scheduling ensures that the change is executed at a time that minimizes impact on operations.

6.1 Resource Allocation and Training Requirements
Identify and allocate the necessary resources, including personnel, technology, and financial resources. Determine training needs to ensure that all stakeholders are prepared for the change.

6.2 Monitoring and Controlling the Change Process
Ongoing monitoring of the change process allows for adjustments as needed to ensure the change is implemented as planned. Control mechanisms help in managing deviations from the plan.

6.3 Documentation and Record Keeping
Maintain detailed records of the change process, including decisions made, steps taken, and outcomes achieved. Documentation supports future audits and reviews, ensuring accountability and learning for future changes.

7. Testing and Quality Assurance

Testing Strategies for Different Types of Changes
Develop tailored testing strategies for each type of change, ranging from unit and integration testing for small scale adjustments to full regression and user acceptance testing for major updates, ensuring comprehensive coverage and minimizing the risk of unintended consequences.

7.1 Criteria for Successful Implementation
Define clear, measurable criteria for each change's success, including performance benchmarks, user satisfaction levels, and adherence to scheduled timelines. These criteria should be established during the planning phase and used as a baseline for evaluation post implementation.

7.2 Handling of Failures and Rollbacks
Establish protocols for quickly identifying failures post implementation and executing rollback plans to revert to the previous state, minimizing operational disruptions. Additionally, conduct thorough analyses of failures to extract lessons learned and refine future change processes.

8. Post Implementation Review/ Monitoring Plan.

8.1 Evaluation of Change Outcomes against Objectives
After the implementation of a change, evaluate its outcomes against the predefined objectives and success criteria. This assessment should consider both quantitative and qualitative measures to determine the change's effectiveness and impact on operations.

8.2 Lessons Learned and Feedback Mechanisms
Document lessons learned during the change process, including what worked well and areas for improvement. Establish feedback mechanisms to gather insights from stakeholders involved in or affected by the change, facilitating a comprehensive understanding of its implications.

8.3 Continuous Improvement Process
Integrate the insights gained from the evaluation and feedback into a continuous improvement process. This involves updating policies, procedures, and practices to enhance future change management efforts, ensuring that the organization remains adaptive and responsive to new challenges and opportunities.

9. Communication Strategy

9.1 Internal and External Communication Plans
The policy to outline distinct strategies for communicating changes internally within the organization and externally to stakeholders and customers. Internally, the plan to utilize emails, intranet postings, and team meetings to ensure all employees are informed. Externally, communication may involve press releases, social media updates, and direct emails to clients, ensuring transparency and maintaining trust.

9.2 Change Announcement Templates and Channels
Templates for announcing changes to be standardized to include the purpose of the change, expected benefits, and any required actions from recipients. Channels for announcements to be selected based on the audience, such as email for internal changes and social media or press releases for external stakeholders.

9.3 Feedback Collection and Response Mechanism
Mechanisms for collecting feedback to be implemented, including surveys, feedback forms, and open forums, allowing stakeholders to express concerns or suggestions. A designated team to review feedback, respond appropriately, and integrate valuable insights into continuous improvement processes.

10. Policy Review and Updates

10.1 Scheduled Reviews and Adhoc Amendments
Regular, scheduled reviews of the policy ensure it remains relevant and effective. Adhoc amendments might be necessary in response to significant changes in regulatory requirements, operational challenges, or technological advancements.

10.2 Documentation of Changes to the Policy
All changes to the policy should be documented, including a summary of the changes, the rationale behind them, and the date of implementation. This ensures transparency and traceability.

10.3 Communication of Policy Updates
Updates to the policy should be communicated to all stakeholders through established channels. This could include internal meetings, email announcements, or updates on the company intranet, ensuring that everyone is aware of the changes and understands our implications.

11. IT Strategy Committee: Outsourced Operations Policy

The IT Strategy Committee plays a critical role in managing and overseeing the outsourced operations within IITL. This points outlines the responsibilities and actions the Committee must undertake to ensure effective governance and risk management for outsourced processes.

1. Governance Mechanism: Establish comprehensive governance structures, including risk-based policies and procedures, to identify, measure, monitor, and control outsourcing risks.
2. Approval Authorities: Define clear approval hierarchies based on the nature and materiality of outsourcing risks.
3. Outsourcing Risk Management: Develop robust outsourcing risk management policies and procedures that reflect the complexity and scope of outsourcing arrangements.
4. **Due Diligence Policy** :- In case of outsourcing arrangements, Develop a proper process note of the due diligence process and conduct a proper due diligence before we onboard any vendor.
5. Periodic Review: Regularly evaluate outsourcing strategies and review all existing material outsourcing agreements to ensure they remain aligned with organizational goals.

6. Risk and Materiality Evaluation: Assess the risks and materiality of prospective outsourcing initiatives, using frameworks established by the Board.
7. Policy Effectiveness Review: Systematically review the effectiveness of outsourcing policies and procedures.
8. Risk Communication: Report significant outsourcing risks to IITL's Board periodically.
9. Independent Review and Audit: Conduct independent audits of outsourced operations to ensure compliance with established policies and procedures.
10. Contingency Planning: Develop and periodically test contingency plans for outsourced operations.
11. Business Continuity Management: Ensure business continuity management practices are in place and verify that outsourced service providers maintain adequate business continuity preparedness.
These points indicate the IT Strategy Committee to implement these guidelines diligently to mitigate risks associated with outsourcing and to uphold the operational integrity and regulatory compliance of IITL's outsourced activities.

12. Appendix

12.1 Change Request Form Template

FORM "A" Change Request Form

S.No.	Particular	Response
1.	**Title of Change Request**	Brief title for the change.
2.	**Requestor Information:**	Name, department, contact info.
3.	**Date of Submission:**	When the request is made.
4.	**Change Description:**	Detailed description of the proposed change
5.	**Rationale/Justification:**	Why the change is necessary
6.	**Expected Impact:**	Anticipated effects on operations, systems, and stakeholders.
7.	**Affected Systems/Departments**	List all that apply.
8.	**Proposed Implementation Date**	Suggested timeline.
9.	**Resource Requirements:**	Any resources needed for the change.
10.	**Approval Signatures**	

12.2 Risk Assessment Tool Template

FORM "B" Risk Assessment Tool Templates

S.No.	Particular	Response
1.	**Risk Identifier**	A unique ID for tracking.
2.	**Risk Description**	Detailed explanation of the risk
3.	**Likelihood Rating**	Scale (e.g., Low, Medium, High).
4.	**Impact Rating:**	Scale (e.g., Low, Medium, High).

5.	**Mitigation Strategies**	Proposed actions to reduce risk
6.	**Responsible Person:**	Who is in charge of managing the risk.
7.	**Monitoring Plan:**	How the risk to be monitored over time.

12.3 Contact Information Template

S.No.	Particular	Response
1.	**Name**	Full name of the key personnel.
2.	**Role**	Job title within the change management process
3.	**Department:**	Specific department or unit.
4.	**Contact Number:**	Work phone number
5.	**Email Address**	Work email address.

13. Policy Approval by the Board of Directors

The policy must be presented to the Board of Directors for review, discussion, and approval. This step ensures that the policy aligns with the organization's strategic objectives and governance standards. The board's approval signifies organizational commitment to the policy.

Conclusion

This policy framework is designed to ensure that changes within the IITL are managed effectively, with minimal disruption to operations and in compliance with regulatory requirements. It emphasizes the importance of clear communication, rigorous assessment, and comprehensive documentation, fostering a culture of continuous improvement and adaptability.