BUSINESS CONTINUITY PLAN

&

DISASTER RECOVERY

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.1	08-11-2023
V.2	23-05-2026
Recommended By	CEO NBFC
Approved By	Board – Meeting Dated 23-05-2026

1. Purpose

This Policy establishes the framework by which IITL will maintain critical operations during and after disruption and restore technology, data, people, facilities and third-party services within defined recovery objectives. It is proportionate to IITL's size, business model and technology footprint and is intended to protect customers, financial records, regulatory reporting, lending/collection operations and other essential services.

2. Scope

- All employees, directors, contractors and relevant service providers involved in critical operations.
- All critical applications, databases, networks, endpoints, cloud services and communication systems.
- Customer, loan, accounting, financial, statutory, regulatory, HR and other records necessary for continuity.
- Primary office, remote/alternate working, backup infrastructure, DR arrangements and critical outsourced services.
- Cyber incidents, system failures, utility outages, fire, flood, natural disasters, telecommunications failures, vendor outages and other material disruptions.

3. Regulatory & Governance Basis

This Policy shall be read with applicable RBI requirements for NBFCs, IITL's Cyber Security Policy, Information Security Policy, Cyber Crisis Management Plan, outsourcing/vendor framework and DPDP/privacy framework. The RBI technology-resilience framework requires robust recovery arrangements, defined RTO/RPO, periodic backup restoration/testing and DR drills for critical information systems where applicable.

The Board approves and oversees this Policy. Senior Management implements it and ensures adequate resources. Detailed recovery runbooks, contact lists and operational procedures shall be maintained as controlled documents under this Policy.

RTO (Recovery Time Objective - Maximum acceptable time to restore a system/process after disruption), in short, how fast do we recover?
RPO (Recovery Point Objective - Maximum acceptable amount of data that can be lost, measured in time), in short, how much data can we afford to lose?

4. Objectives

- Ensure timely continuation of critical business services.
- Protect life, employees, customers, data and assets.
- Minimise financial, operational, legal, regulatory and reputational impact.
- Restore critical technology and data within approved RTO/RPO.
- Provide resilient remote/alternate working arrangements.
- Maintain effective crisis communication and escalation.
- Meet applicable regulatory/statutory obligations.
- Validate readiness through periodic testing and remediation.

5. Governance & Responsibilities

Role	Responsibility
Board	Approve/review policy; oversee material resilience risks, test results, major gaps and significant disruptions.
CEO / Senior Management	Activate BCP/DR where warranted; prioritise services; allocate resources and approve major recovery decisions.
BCP-DR Coordinator	Maintain BCP/DR framework, BIA, contacts, test calendar, plans and issue register.
IT In-Charge / CISO	Technology recovery, backups, DR infrastructure, cyber resilience, restoration, access and technical communications.

Business Process Owners	Identify critical processes, dependencies, minimum resources, workarounds and priorities.
Compliance / Legal	Regulatory/statutory obligations, notifications and legal communications.
Finance / Treasury	Banking, liquidity, payments, accounting and financial records.
HR / Administration	Employee welfare, alternate workplace, facilities, supplies and communications.
Vendors	Continuity, DR, support, escalation and incident notification.
Employees	Follow instructions, preserve records and report disruptions promptly.

6. Business Impact Analysis (BIA)

IITL shall maintain a documented BIA at least annually and whenever there is a material change. It shall identify critical processes, dependencies, maximum tolerable downtime, RTO, RPO, minimum staffing, systems/data, workarounds and vendors.

Business Function	Priority	Indicative RTO	Indicative RPO
Loan/customer servicing	Critical	≤4 hours	≤1 hour
Collections/payment processing	Critical	≤4 hours	≤1 hour
Accounting/financial reporting	Critical	≤8 hours	≤4 hours
Regulatory/statutory reporting	Critical/High	As required	≤24 hours
Treasury/banking	Critical	≤4 hours	≤1 hour
Email/communications	High	≤8 hours	≤4 hours
HR/payroll	Medium	≤48 hours	≤24 hours
Administrative systems	Medium/Low	≤72 hours	≤24–48 hours

7. Critical Services & Minimum Capability

- Customer servicing and communications.
- Loan administration and receipt accounting.
- Banking/payment access.
- Protection and availability of customer/loan records.
- Financial accounting and regulatory reporting.
- Management communications and decision-making.
- Cybersecurity monitoring and incident response.
- Minimum employee capability and critical-role coverage.

8. Continuity Strategies

- Secure remote working using approved devices and access mechanisms.
- Alternate workplace arrangements where remote working is inadequate.
- Cloud/hosted redundancy and vendor DR where applicable.
- Segregated/immutable backup copies where appropriate.
- Manual fallback procedures for critical processes.
- Cross-training and designated alternates.
- Multiple crisis communication channels.
- Critical vendor escalation and substitute arrangements where feasible.
- Predefined recovery priorities.

9. Disaster Recovery Strategy

- Maintain recovery arrangements appropriate to technology criticality.
- Document primary/recovery environments, dependencies, connectivity, configurations and restoration sequence.
- Maintain protected backups of critical data and configurations.

- Periodically test restoration.
- Patch, secure and validate recovered systems before production use.
- Maintain DR runbooks with prerequisites, sequence, owners and contacts.
- Review DR commitments/evidence for critical third parties.

10. Backup & Data Recovery

Control	Minimum Requirement
Frequency	Risk-based and aligned to approved RPO
Protection	Access controlled and protected from unauthorised alteration/deletion
Off-site/segregated copy	For critical data where technically appropriate
Restoration testing	Periodic restore tests with evidence
Retention	Legal, regulatory and business requirements
Encryption	Where appropriate to sensitivity/risk
Monitoring	Backup failures reviewed promptly
Validation	Completeness, integrity and application usability checked

11. Alternate Workplace / Remote Working

- Maintain capability for critical functions from approved remote/alternate locations.
- Remote access shall comply with Cyber Security and Information Security Policies.
- Only authorised personnel may access systems remotely.
- Critical staff shall have alternates and contact methods.
- Confidential information shall not be transferred to unauthorised personal devices/accounts.
- Alternate arrangements shall be tested periodically.

12. Activation Criteria

- Loss of primary office/infrastructure.
- Material outage of critical IT/telecommunications.
- Cyberattack/ransomware affecting critical operations.
- Extended power/network outage.
- Major vendor failure.
- Natural disaster, fire, flood or physical event.
- Unavailability of key personnel.
- Any event reasonably expected to breach RTO or materially affect customers/regulatory obligations.

13. Activation & Escalation

The CEO or authorised Senior Management official may activate BCP/DR. In a cyber crisis, activation shall be coordinated with the Cyber Crisis Management Plan. If the CEO is unavailable, the designated alternate shall act under the delegation matrix.

Detect and log the disruption.
Assess people, premises, technology, data, customers and operations.
Determine whether contingency measures are sufficient.
Activate the relevant BCP/DR plan and notify recovery teams.
Prioritise critical services and recovery sequence.
Escalate to management/Board according to severity.
Coordinate external/regulatory notifications where applicable.

14. BCP/DR Phases

Phase	Key Activities
I – Preparedness	BIA, risk assessment, inventories, backups, contacts, alternate arrangements, training and testing.
II – Activation	Assess event, declare activation, notify teams, establish command and prioritise services.
III – Continuity & Recovery	Remote/alternate operations, system/data restoration, workarounds, customer communication and backlog management.
IV – Return to Normal	Validate primary environment, migrate safely, reconcile data/transactions and close temporary arrangements.
V – Lessons Learned	Post-event/test review, root cause, improvements, owners and closure tracking.

15. Emergency Response & Safety

- Life safety takes priority over asset recovery.
- Follow evacuation/emergency/authority instructions.
- Do not enter unsafe premises to retrieve records/equipment.
- Access affected premises only when authorised and safe.
- Retrieve vital material only when safe and legally permitted.
- Maintain employee welfare and accountability.

16. Recovery Teams

Team	Primary Duties
Crisis Management Team	Overall decisions, activation, prioritisation and stakeholder management.
IT/DR Recovery Team	Infrastructure, applications, connectivity, backup and restoration.
Business Recovery Team	Critical processes, workarounds, customer servicing and backlog.
Finance/Treasury	Payments, banking, liquidity, accounting and reconciliation.
HR/Admin	People, alternate workplace, facilities, supplies and communications.
Legal/Compliance	Regulatory/statutory notifications and legal risk.
Vendor Coordination	Third-party escalation and service recovery.

17. Crisis Communications

- Maintain current primary and alternate contacts.
- Use two independent communication channels where feasible.
- Only authorised personnel may issue external statements.
- Customer communications shall be accurate and proportionate.
- Regulatory communications shall be made by designated officials.
- Material decisions and communications shall be documented.

18. Critical Records

- Customer/loan records
- Accounting/financial records
- Banking/payment records
- Regulatory/statutory records
- Material contracts/vendor records
- Insurance records
- Corporate/legal records
- System configurations and recovery information
- BCP/DR plans, contacts, tests and incidents

19. Cyber Incident / Ransomware Continuity

Cyber incidents shall be managed under the Cyber Security Policy and CCMP, with BCP/DR activated where business services are materially affected. Systems shall be isolated as appropriate, evidence preserved, backups protected, compromised credentials reset and restoration performed only from trusted sources after security validation. Applicable RBI/CERT-In/DPDP reporting shall be assessed and completed within prescribed timelines.

20. Third-Party Continuity & Outsourcing

- Identify critical outsourced services and dependencies.
- Obtain documented BCP/DR capability from material vendors where relevant.
- Contracts should address continuity, incident notification, recovery, audit/access and exit as appropriate.
- Obtain proportionate assurance/evidence of critical vendor resilience.
- Maintain alternatives for critical single points of failure where feasible.
- Include critical vendors in relevant exercises.

21. Testing & Drills

IITL shall maintain a formal BCP/DR testing programme. Critical technology recovery/DR shall be tested at least as frequently as applicable RBI requirements and at least half-yearly for critical information systems where required. Tests shall validate actual recovery and business continuity, not merely document review.

Test	Minimum Expectation
Table-top	At least annually; scenario-based management exercise
IT restore	Periodic restoration of critical backups
DR drill	At least half-yearly for critical information systems where applicable
Remote-working	At least annually or after material change
Communications	At least annually
Critical vendor continuity	Risk-based; periodically for critical vendors
Integrated BCP exercise	At least annually where proportionate

22. DR Test Success Criteria

- Critical systems restored within RTO.
- Data loss within RPO.
- Critical business processes performed end-to-end.
- Required staff/alternates can access systems.
- Communication/escalation channels work.
- Security controls remain effective in recovery.
- Material gaps have corrective actions.

23. Return to Primary Operations

- Confirm primary site/system readiness and security.
- Obtain authorized management approval.
- Schedule migration/cutover.
- Reconcile contingency-period transactions and data.
- Validate accounting, customer/loan records and regulatory data.
- Restore normal access/routing.
- Securely decommission temporary resources and secure records.
- Close activation after business-owner confirmation.

24. Post-Test / Post-Incident Review

- Document timeline and decisions.
- Assess customer, financial, operational and regulatory impact.
- Identify root cause and control gaps.
- Assess RTO/RPO performance.
- Assign corrective actions and owners.
- Update BIA, recovery strategies, runbooks and training.
- Report material issues to Senior Management and Board/appropriate forum.

25. Evidence & Records

- Approved policy
- BIA/critical-process register
- System inventory
- RTO/RPO register
- Recovery runbooks
- Backup/restore records
- DR drill reports
- Table-top reports
- Remote-working tests
- Vendor continuity evidence
- Emergency contacts
- Incident/activation logs
- Corrective-action tracker
- Board/management reports

26. Exceptions

Any deviation from an approved recovery objective or mandatory control shall be documented with reason, risk, compensating measure, approving authority, validity period and remediation plan. Regulatory requirements cannot be waived through an ordinary internal exception.

27. Review & Amendment

This Policy shall be reviewed at least annually and after a major disruption, material BCP/DR test, cyber crisis, significant technology/business change, critical outsourcing change or regulatory amendment. Material amendments shall be placed before the Board.

Appendix A – Critical Process BIA Template

Process	Owner	Criticality	RTO	RPO	Min. Staff	Systems	Dependencies	Workaround
Loan/customer servicing		Critical						
Collections/payment processing		Critical						
Accounting/financial reporting		Critical						
Regulatory reporting		Critical/High						
Banking		Critical						

Appendix B – Emergency Contact Matrix

Role / Organization	Primary	Alternate	Contact Details
CEO			
BCP-DR Coordinator			
IT / DR Lead			
Security Lead			
Finance			
Compliance / Legal			
HR / Administration			
Critical IT Vendor			
Banking Partner			

Appendix C – Minimum DR Drill Report

Item	Details
Scenario	
Date/time	
Participants	
Systems/processes	
RTO achieved	
RPO achieved	
Data reconciliation	
Issues/gaps	
Corrective actions	
Owner/due date	
Management sign-off	