THE MAHAVEER CO-OP. BANK LTD., BELAGAVI

BCDR POLICY

POLICIES FOR THE FY
2026-27
https://mahaveerbank.bank.in

Approved by the Board of Directors at its meeting held on 23/6/26, vide Resolution No. 11.

1. Introduction

This Business Continuity and Disaster Recovery (BCDR) Policy is prepared based on the guidelines, circulars and instructions issued by the Reserve Bank of India (RBI) from time to time and should be read along with them.

The main purpose of this policy is to make sure that the Bank's important services continue without interruption as much as possible, and in case of any disruption, the systems and operations can be restored quickly. It also aims to protect the Bank's data by maintaining its confidentiality, integrity and availability.

This policy is framed keeping in mind the RBI guidelines applicable to Urban Co-operative Banks and also considering general best practices for business continuity and risk management

2. Objective

• To ensure that the Bank's important operations continue smoothly during and after any disruption, so that customer service and regulatory requirements are not affected.

• To reduce losses, system downtime, data issues, and reputational risk that may arise due to system failures, cyber-attacks, natural disasters, pandemics, or other unexpected events.

• To put in place a clear and structured system for business continuity and disaster recovery, including preventive measures, recovery plans, and defined timelines for restoring systems and services.

• To protect customer information by maintaining confidentiality, integrity, and availability of data, and to ensure proper communication with all concerned during any crisis.

• To improve the Bank's preparedness by conducting regular testing, training, and awareness, and by continuously strengthening its response and recovery process.

3. Scope

This policy is applicable to the following:

- All branches and administrative offices of the Bank.
- All departments and employees of the Bank.
- Core Banking System (CBS) and all related IT systems, applications, and infrastructure.
- Data Centre, Disaster Recovery (DR) site, and network systems.

- Payment systems such as NEFT, RTGS, IMPS, UPI, and other digital services.
- All third-party service providers, vendors, and outsourced agencies.
- Any other persons or entities involved in the Bank's critical operations.

This policy shall be followed by all concerned, both internal and external, to ensure proper continuity, safety, and smooth functioning of the Bank's operations.

4. Definitions

•Business_Continuity_(BC):
The ability of the Bank to continue its important services without interruption, even during situations like natural disasters, cyber-attacks, or system failures. It involves proper planning in advance to keep essential operations running.

•Disaster_Recovery_(DR):
The process of restoring IT systems, data, and infrastructure after a major disruption so that normal operations can start again. It mainly focuses on recovery of technology and systems.

•Recovery_Time_Objective_(RTO):
The maximum time within which a system or activity should be restored after a disruption. It shows how long the Bank can manage without that system or service.

•Recovery_Point_Objective_(RPO):
The maximum amount of data loss the Bank can accept in case of a disruption. It indicates up to what point the data should be recovered (for example, last 2 hours data).

•Critical_Functions:
The most important activities of the Bank that must continue or be restored quickly, such as core banking services, customer transactions, and fund transfers.

•Disruption:
Any event that affects normal banking operations, such as system failure, cyber-attack, power failure, natural disaster, or similar situations.

5. Roles and Responsibilities

Function	Responsibility
Board of Directors	Approves BCDR policy and reviews implementation.
BCDR Committee	Monitors risk, reviews BC plans, and conducts drills.

IT Department	Maintains DR infrastructure and ensures recoverability.
Branch Heads	Ensure local continuity procedures are known and followed.
All Staff	Must be familiar with emergency procedures and escalation.

Risk Assessment & Business Impact Analysis (BIA)

The bank shall conduct periodic risk assessments to identify potential threats. Illustrative categories, examples, and mitigation strategies are as follows

Type	Examples	Solution in Banking Data
Natural Disasters	Earthquakes, floods, landslides, wildfires, pandemics	Off-site data storage, geo-redundant DR sites, remote access for critical staff, cloud backups
Man-Made Disasters	Terrorism, war, urban fires, building collapse	Secure data centers in low-risk zones, strong physical security, redundant power and communication lines
Cyber Threats	Hacking, ransom ware, phishing, malware attacks, data breaches	Firewalls, IDS/IPS, endpoint security, regular patching, employee awareness, data encryption, SOC monitoring
Technical Failures	Hardware crash, server failure, database corruption, software bugs	Redundant servers, failover systems, regular backups, system monitoring tools
Power & Utility Failures	Power outages, UPS failure, cooling system breakdown	UPS systems, generators, dual power sources, environmental monitoring systems
Network & Connectivity Issues	ISP failure, network congestion, telecom outages	Multiple ISP links, network redundancy, SD-WAN, backup communication channels
Human Errors	Accidental data deletion, misconfiguration, operational mistakes	Maker-checker controls, access restrictions, training, audit trails, automated validation checks

6. Key Components of the BCDR Policy

The Bank's Business Continuity and Disaster Recovery (BCDR) Policy includes the following main parts to ensure proper preparedness, response, and recovery during any disruption.

6.1 Business Impact Analysis (BIA)

- Identification of critical business functions, services, systems, and supporting infrastructure.
- Determination of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each critical function.
- Prioritization of recovery activities based on the severity of operational, financial, legal, and reputational impacts.

6.2 Risk Assessment

- Evaluation of potential internal and external threats, including but not limited to fire, flood, cyber-attacks, power outages, pandemics, and supply chain disruptions.
- Assessment of the likelihood and potential impact of each identified risk.
- Implementation of appropriate risk mitigation strategies, preventive controls, and contingency measures to minimize vulnerabilities.

6.3 Business Continuity Plan (BCP)

- Documented and actionable procedures to maintain or resume critical business operations during and after a disruption.
- Strategies for alternate site operations, manual transaction processing, and continuity of customer services.
- Clearly defined roles and responsibilities, escalation matrix and updated contact details of key personnel.
- Communication plan to effectively inform customers, regulators, vendors, and internal stakeholders during crisis situations.

6.4 Disaster Recovery Plan (DRP)

- IT-specific procedures for recovery and restoration of critical technology infrastructure and services, including Core Banking System (CBS), servers, email systems, internet banking, and communication systems.
- Defined backup strategy covering frequency, storage (onsite/offsite/cloud), validation, and restoration procedures.

- Establishment of a Disaster Recovery (DR) site, either offsite or through an external service provider, along with clearly defined activation criteria.
- Specification of RTO and RPO for each critical IT system to ensure timely and effective recovery.

7. Backup Policy

The Bank shall maintain proper and secure data backup arrangements to ensure that data is safe and can be recovered in case of system failure or any other issue. The main points are as follows:

• All important data, customer details, and system information shall be backed up daily.

• Different types of backups like full and incremental may be used for better storage and easy recovery.

• Backup data shall be stored at other locations such as DR site or in safe offline storage. Cloud backup may also be used.

• Backup data shall be kept secure using proper protection methods to avoid unauthorized access.

• Backup data shall be checked regularly to make sure it can be restored properly when required.

• Access to backup data shall be given only to authorized staff.

• Backup data shall be kept for a period as per RBI guidelines and Bank's policy.

8. Alternate Site Readiness

To ensure that important operations continue during any disaster or major issue, the Bank shall maintain a Disaster Recovery (DR) site with the following:

• The DR site shall be set up in a different location to avoid impact from the same event.

• It should be able to take over Core Banking System (CBS) and other important systems when required.

• The site shall have proper systems, network, power backup, and other necessary facilities.

• The connection and working of the DR site shall be tested at least once in a year to ensure it is ready for use.

9. Testing and Drills

To ensure the effectiveness and readiness of the Bank's Business Continuity and Disaster Recovery arrangements, the following practices shall be adhered to:

- **Business Continuity Plan (BCP)** and **Disaster Recovery (DR)** drills shall be conducted **at least twice a year** to test the robustness of response mechanisms.
- Drills shall be designed to **simulate various failure scenarios**, including system outages, cyber incidents, and physical disruptions, to evaluate the Bank's preparedness across functions.
- **Observations, gaps, and lessons learned** during each drill shall be **documented** and used to review and enhance the BCDR policies and procedures.
- **Post-drill reports** shall be prepared and, where applicable, **submitted to the Board of Directors** and **Reserve Bank of India (RBI)** in compliance with regulatory requirements.

10. Communication Strategy

Clear and timely communication is very important during any disruption to avoid confusion and to maintain confidence. The Bank shall have a proper Crisis Communication Plan with the following:

•Internal_Communication:
Information shall be shared promptly with all employees, branches, and teams so they understand their roles and can continue operations smoothly.

•External_Communication:
Proper communication shall be maintained with customers, service providers, and regulators, with clear updates on the issue, actions taken, and expected restoration time.

•Predefined_Templates:
Standard formats for messages, emails, SMS, and notices shall be kept ready in advance. This will help in sending quick, clear, and consistent communication during emergency situations without delay.

11. Training and Awareness

To ensure preparedness and effective response during disruptions, the Bank shall implement a structured training and awareness program as part of its BCDR framework. Key elements include:

- **Regular_Training_Programs:**
  Periodic training sessions for all employees to familiarize them with Business Continuity and Disaster Recovery (BCP/DR) procedures, individual responsibilities, and response protocols.
- **Induction_for_New_Employees**:
  BCP/DR awareness shall be an integral part of the onboarding process to ensure that all new staff are informed about the Bank's continuity framework from the outset.

- **Awareness_Campaigns:**
  Ongoing awareness initiatives covering topics such as physical security, incident reporting and escalation procedures, emergency contacts, and first-response actions during a crisis.

12. Review and Governance

Effective governance and periodic review are essential to ensure that the Business Continuity and Disaster Recovery (BCDR) Policy remains aligned with the Bank's evolving risk environment, regulatory landscape, and operational needs. The following measures shall be adopted:

- The BCDR Policy shall be **reviewed at least once annually** or earlier in response to:
  - **Significant changes** in IT infrastructure, including system upgrades, migrations, or the adoption of new technologies.
  - **Updates in regulatory guidelines** issued by the Reserve Bank of India (RBI) or other relevant authorities.
  - **Material changes in business operations**, such as the introduction of new products/services, branch expansions, or changes in delivery channels.
- The **review process** shall include:
  - Evaluation of the effectiveness of current BCDR controls and procedures.
  - Consideration of feedback from BCP/DR drills, audits, and incident reports.
  - Identification of gaps, emerging threats, and opportunities for improvement.
- Outcomes of the review, including proposed updates or enhancements, shall be:
  - **Formally documented** with detailed justifications.
  - **Presented to and approved** by the Bank's Board of Directors or a designated committee overseeing risk and compliance.
- The Board shall provide **strategic oversight** to ensure that BCDR governance remains robust, compliant, and in line with industry best practices.

13. Compliance and Audit

To ensure the effectiveness, integrity, and regulatory compliance of the Bank's Business Continuity and Disaster Recovery (BCDR) framework, the following measures shall be implemented:

- The Internal Audit Department shall conduct an annual review and verification of the Bank's BCP and DR preparedness, including assessment of documentation, infrastructure readiness, testing outcomes, and staff awareness.

- Any identified non-compliance, deficiencies, or gaps shall be reported to the senior management and must be rectified within 30 days or within a time frame as deemed appropriate by the Audit Committee.
- All BCDR-related documents, including policies, test reports, drill observations, incident logs, and review records, shall be maintained securely in accordance with the Bank's data retention policy and shall be readily accessible for internal and regulatory audits.
- The Bank shall also ensure compliance with applicable guidelines issued by the Reserve Bank of India (RBI) and other regulatory bodies concerning business continuity and disaster recovery.

14. Vendor and Outsourcing Considerations

The Bank recognizes the importance of ensuring business continuity not only within its internal operations but also across outsourced services and third-party vendors. Accordingly, the following standards shall be enforced:

- All critical third-party service providers and vendors engaged in supporting the Bank's essential functions must maintain and demonstrate adequate Business Continuity and Disaster Recovery (BCDR) capabilities.
- All Service Level Agreements (SLAs) with such vendors must incorporate specific provisions related to disaster management, including clearly defined response times, recovery time objectives (RTOs), and recovery point objectives (RPOs).
- The BCDR plans and capabilities of critical vendors shall be reviewed and assessed at least annually to ensure their continued alignment with the Bank's risk tolerance, operational dependencies, and regulatory expectations.
- In case of any significant changes to a vendor's BCDR framework or reported incidents affecting their service delivery, the Bank shall initiate an immediate review and may seek corrective measures or alternative arrangements as needed.

15. Policy Enforcement

Compliance with the Business Continuity and Disaster Recovery (BCDR) Policy is mandatory for all employees, departments, and relevant stakeholders of the Bank. Any instance of **non-compliance** shall be taken **seriously** and may result in:

- **Disciplinary action**, in accordance with the Bank's internal code of conduct and human resource policies.
- **Review and escalation** to senior management and/or the designated Risk Management Committee for further evaluation and corrective measures.

The Bank reserves the right to take appropriate action to ensure that all personnel and service providers adhere to the provisions of this policy as part of its overall governance and risk management framework.

The Mahaveer Co-operative Bank Ltd., Belagavi

Chief Executive Officer/Vice-Chairman/Chairman

THE MAHAVEER CO-OP. BANK LTD. BELAGAVI