Business Continuity and Disaster Recovery (BCDR) Policy 2025-26

Approved by the Board of Directors at its meeting held on 29-07-2025, vide Resolution No. 10.

1. Preamble

This Business Continuity and Disaster Recovery (BCDR) Policy shall be read in conjunction with, and is subject to, the applicable guidelines, circulars, and notifications issued by the Reserve Bank of India (RBI), as amended from time to time. The policy outlines the Bank's commitment to ensuring uninterrupted service delivery, safeguarding of critical data, and rapid restoration of operations in the event of any major disruption. It has been framed in compliance with the RBI's guidelines applicable to Urban Co-operative Banks and is aligned with established industry standards for operational resilience and risk management

---

2. Objective

- To ensure uninterrupted functioning of critical banking operations during and after any disruptive incident, thereby maintaining customer confidence and regulatory compliance.
- To minimize potential financial losses, operational downtimes, data breaches, and reputational damage resulting from system failures, cyber-attacks, natural calamities, pandemics, or any other unforeseen events.
- To establish a comprehensive and structured framework for disaster recovery, including preventive controls, recovery strategies, and clearly defined timelines for the restoration of IT systems, business services, and infrastructure.
- To safeguard customer data, maintain data integrity, and ensure timely communication with stakeholders during crisis situations.
- To promote a culture of preparedness through regular testing, training, and continuous improvement of the Bank's resilience and response capabilities.

---

3. Scope

This policy is applicable to all branches, departments, employees, IT systems, data centres, service providers, and other stakeholders involved in the Bank's critical functions and infrastructure. It shall be adhered to by all internal and external entities responsible for maintaining the continuity, security, and resilience of banking operations.

---

4. Definitions

- **Business Continuity (BC):**
  The capability of the Bank to ensure uninterrupted delivery of critical products and services to customers at acceptable predefined levels, even during adverse events such as natural disasters, cyber-attacks, system failures, or other disruptions. It involves proactive planning to maintain essential operations and manage risks effectively.
- **Disaster Recovery (DR):**
  A coordinated process involving the restoration of IT systems, infrastructure, applications, and data to ensure the resumption of normal business functions following a significant disruption or disaster. Disaster Recovery is a key component of the broader Business Continuity framework and focuses specifically on technology recovery.
- **Recovery Time Objective (RTO):**
  The maximum permissible duration within which a business process or IT system must be restored after a disruption to avoid unacceptable operational, financial, or reputational impact. It defines the Bank's tolerance for downtime of specific functions or systems.
- **Recovery Point Objective (RPO):**
  The maximum tolerable period in which data might be lost due to a major incident. It represents the point in time to which data must be recovered after a disaster (e.g., data backed up within the last 2 hours) to ensure business continuity with minimal loss.
- **Critical Functions:**
  The core business processes and services that are essential to the Bank's operations and must be prioritized for continuity and recovery during and after a disruption (e.g., core banking services, customer transactions, fund transfers).
- **Disruption:**
  Any event—planned or unplanned—that causes interruption or degradation of normal banking operations, such as hardware/software failure, cyber-attack, power outage, natural disaster, or pandemic.

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.

Type	Examples	Solution in Banking Data
Natural Disasters	Earthquakes, Landslides, Floods, Wildfires, Pandemics	Data stored at off-site locations, data replication across multiple branches, remote access for critical staff
Man-Made Disasters	Terrorism, War, Urban fires, Building collapses	Secure data centers in safe zones, strong cybersecurity protocols, redundant power and communication lines

6. Key Components of the BCDR Policy

The Bank's Business Continuity and Disaster Recovery (BCDR) Policy comprises the following core components to ensure preparedness, response, and recovery from any disruptive events:

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 impact.

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 risk mitigation strategies, preventive controls, and contingency measures to reduce 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 relocation, manual transaction processing, and continuity of customer services.
- Clear roles and responsibilities, escalation protocols, and updated contact details of key personnel.
- Communication plans to inform customers, regulators, vendors, and internal stakeholders during crisis situations.

6.4 Disaster Recovery Plan (DRP)

- IT-specific procedures for recovering and restoring essential technology infrastructure and services, including:
    - Core Banking System (CBS), servers, email, internet banking, ATM/POS switching, and network systems.
- Backup strategy including frequency, storage, validation, and restoration procedures.
- Defined Disaster Recovery (DR) site—either offsite or hosted by an external service provider—with criteria for its activation.
- RTO and RPO defined for each critical IT system to ensure timely and effective recovery.

---

7. Backup Policy

The Bank shall maintain a robust data backup policy to ensure data integrity, availability, and recoverability in the event of a system failure or disaster. Key elements include:

- All critical business and customer data shall be backed up on a daily basis and stored in a secure manner to prevent data loss or corruption.
- A combination of full, incremental, and differential backup methods shall be used to optimize storage and recovery efficiency.
- Backup copies shall be retained at offsite and offline locations, including air-gapped storage or secure cloud environments with end-to-end encryption.
- Regular testing and validation of backup data shall be conducted to ensure successful restoration and the reliability of backup procedures.

---

8. Alternate Site Readiness

To ensure uninterrupted continuity of critical operations during a disaster or major disruption, the Bank shall maintain a fully functional Disaster Recovery (DR) site with the following requirements:

- The DR site shall be located in a geographically separate area to mitigate the risk of simultaneous impact from regional disruptions.
- It must be capable of seamlessly taking over the operations of the Core Banking System (CBS) and other mission-critical applications.
- The site shall be equipped with adequate hardware, network infrastructure, power backup, and other essential resources to support full operational functionality.
- Connectivity to the DR site shall be tested at least once every quarter to validate readiness, ensure failover capability, and identify any gaps in performance or response.

---

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

An effective communication strategy is critical to managing disruptions and maintaining stakeholder confidence. The Bank shall establish a comprehensive **Crisis Communication Plan** as part of its BCDR framework, which shall include:

- **Internal Communication:**
  Timely and coordinated communication with employees, branches, and key operational teams to ensure clarity of roles, updates on the situation, and instructions for continued service delivery.
- **External Communication:**
  Structured communication with customers, service providers, regulatory authorities, and other external stakeholders to provide status updates, response measures, and service restoration timelines.
- **Predefined Templates:**
  Development of standard templates for press releases, customer advisories, email alerts, and SMS notifications to ensure consistency, accuracy, and speed of communication during a crisis.

---

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
Sd/-

Chief Executive Officer/Vice-Chairman/Chairman