AU Small Finance Bank Limited

Business Continuity Policy

Background and Scope

1.1 Preamble

Business Continuity Plan (BCP) is a proactive plan to avoid and mitigate risks associated with a disruption of business operations due to any critical scenario. AU small finance Bank's Business continuity management policy is to respond to a Significant Business Disruption by safeguarding employee's life, bank's property, making a financial and operational assessment, quickly recovering, and resuming operations, protecting Bank's records, and allowing customers to transact business with no hindrance. This Business Continuity Plan includes:

- Plans, measures, and arrangements to manage business interruptions to provide continuity of services at a minimum acceptable level and to safeguard bank's financial and competitive position.

- Identification of necessary resources and critical units of the bank to support business continuity, including personnel, information technology, financial allocations, infrastructure protection and accommodations.

Creating and maintaining a BCP help bank to ensure that the bank has the resources and information needed to deal in crisis event. AU small finance bank (the Bank) acknowledges and recognizes the importance of ensuring resiliency in its business operations and maintaining the trust and confidence of its stakeholders, including Customers, regulators, employees, and public at large.

1.2 Key Factors to be Considered for BCP Design

Following factors should be considered while designing the BCP:

- ➢ Probability of unplanned events, including natural or man-made disasters, earthquakes, fire, hurricanes, or bio-chemical disaster.
- ➢ Security threats.
- ➢ Increasing infrastructure and application interdependencies.
- ➢ Regulatory and compliance requirements, which are growing increasingly complex.
- ➢ Failure of key third party arrangements.
- ➢ Globalisation and the challenges of operating in multiple countries.
- ➢ Any other situation.

Objective: The objective of this policy is to ensure that all the employees of the bank should be safe and a proactive response to various contingencies such as site contingency (premise is unavailable, power outage, systems not working, Personnel Unavailable etc.) and city contingency (Strike, riots, act of terrorism, etc.) should be in place. It also Ensure that the bank adheres to Customer, Contractual Legal & Regulatory obligations during any contingency.

Scope: AU Small finance bank's BCP policy applies to **people, facilities, workplaces, business processes, technology, services, and suppliers** that support critical activities under various contingencies as identified through the process of Risk Assessment impacting Operations at the Bank.

1. Roles, Responsibilities and Organizational structure

Board of Directors and Senior management

A bank's Board has the ultimate responsibility and oversight over BCP activity of a bank. The Board approves the Business Continuity Policy of a bank. Senior Management is responsible for overseeing the BCP process which includes*:*

- The Bank's Board of Directors shall be responsible for providing the necessary guidance and direction to enable the development and implementation of an effective Business Continuity Plan (BCP) & framework across the entire bank.
- The Operational Risk Management Committee (ORMC) shall be responsible for ongoing monitoring and review of the Business Continuity Plans (BCP) across the bank. Accordingly, no separate BCP Committee shall be constituted.
- The Operational Risk Management department (ORMD) shall be responsible for co-ordination with various Units to identify the critical business functions and processes across the bank, for which effective Business Continuity Plan needs to be planned for.
- Heads of the Units shall be responsible for documenting the BCP (Business continuity plan) for their respective functions and testing the plan at the defined frequency. Results of the BCP testing shall be submitted to the Operational Risk Management Department who would help in resolution of the identified gaps.
- The National Manager -Operational Risk will be appointed as the BCM (Business continuity Management) Owner/head of the Bank.
- All the BCP drills/exercises will be done under supervision of ORMD- Head. Report of testing will be shared with Operational Risk Management Committee.
- Any deviation before drill, in pre-approved business continuity plan of the business has to approved by the ORMD head and CRO jointly.

2.1 BCP Head or Business Continuity Co-ordinator

A senior official designated as the Head of BCP activity or function.

His or her responsibilities include:

- Developing of an enterprise wide BCP and prioritization of business objectives and critical operations that are essential for recovery.
- Business continuity planning to include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components.
- Periodic updating of business continuity plans based on changes in business processes, audit recommendations, and lessons learned from testing.
- Following a cyclical, process-oriented approach that includes a business impact analysis (BIA), a risk assessment, management and monitoring and testing.
- Considering all factors and deciding upon declaring a "crisis".

2.2 BCP Committee or Crisis Management Team

Since electronic banking has functions spread across more than one department, it is necessary that each department understands its role in the plan. It is also important that each gives its support to maintain it.

Operational Risk Management Committee (ORMC) shall be responsible for ongoing monitoring and review of the Business Continuity Plans (BCP) across the bank. Accordingly, no separate BCP Committee shall be constituted. Crisis Management Team shall be constituted and consisting of senior officials from departments like HR, IT, Legal, Business and Information Security.

To exercise, maintain and to invoke business continuity plan, as needed.

- Department heads determine the activation of the BCP.
- Department head communicate, train, and promote awareness.
- Ensure that the Business Continuity Plan (BCP) fits with other plans and requirement of concerned authorities.
- Ensure training and awareness on BCP to concerned teams and employees.
- Co-ordinating the activities of other recovery, continuity, response teams and handling key decision-making.

- Other functions entail handling legal matters evolving from the disaster and handling public relations and media inquiries.

2. Assumptions/Minimum Requirement

- The BCP strategy agreed upon would be implemented and tested at periodic intervals for its workability.
- There is no possible single risk that could destroy all bank's facilities.
- Staff will be available to perform urgent functions defined within the plan.
- Alternate location is available for processing the organization's work.
- Primary work location and alternate work location are not affected simultaneously.
- Staff can be notified and can report to the alternate location to perform identified activities.
- The continuity plans are maintained with regard to training, testing and updating.
- Surface transportation in the local area is possible, and logistics will be duly taken care of. Bank has Emergency response plan, Pandemic plan, and physical security document in place to address crisis event.

3. BCP Methodology

Phase 1: Business Impact Analysis

- Identification of critical businesses owned and shared resources with supporting functions to come up with the Business Impact Analysis (BIA).
- Formulating Recovery Time Objectives (RTO), based on BIA.
- Identification of the Recovery Point Objective (RPO), for data loss for each of the critical systems and strategy to deal with such data loss.
- Alternate procedures during the time systems are not available and estimating resource requirements.

  Any exception to the decision on the critical business units shall be taken by the CRO in consent with respective departmental heads.

  Refer BIA policy for your reference.

Phase 2: Risk Assessment

- Structured risk assessment based on comprehensive business impact analysis.
- Risk management by implementing appropriate strategy to attain the bank's agreed RTOs and RPOs.
- Impact on restoring critical business functions, including customer-facing systems and payment and settlement systems such as cash disbursements, ATMs, internet banking, or call centers.

Phase 3: Determining Choices and Business Continuity Strategy

- The methodology should prove for the safety and well-being of people in the branch / outside location at the time of the disaster.
- Define response actions based on identified classes of disaster.

Phase 4: Developing and Implementing BCP

- Action plans, i.e., defined response actions specific to the bank's processes, practical manuals and testing procedures.
- Compatibility and co-ordination of contingency plans at both the bank and its service providers.
- Having contingency plans for outsourcing arrangement based on the degree of materiality and dependency of the outsourced vendor.

4. BCP Framework

Appropriate plans and frameworks will be prepared to identify the incidents, communicating the situation to central and respective location, and responding to the procedure of reacting to the incidents.

- **Invocation-**
  At the happening of any disaster or situation where BCP to be invoked, the respective department/branch location/office should duly inform the Operational Risk committee members (If any) or to the ORMD/Chief Risk Officer to initiate the recovery course.

- **Emergency procedures-**
  Actions to be taken for an incident which jeopardises business operations and/ or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g., police, fire service, health-care services and local government.

  Refer ERP for your reference.

- **Pandemic planning-** Pandemics are defined as epidemics, or outbreaks in humans, of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide. Due to their crucial financial and economic role, financial institutions should have plans in place that describe how they will manage through a pandemic event.

  Refer pandemic planning policy for your reference.

- **Recovery objectives-** The recovery objectives will be set in place to react to the unforeseen contingencies immediately which are hampering the business-as-usual activities. In case of occurrence of any incident, designated head of the department will take appropriate action as soon as possible with the support of respective teams.

- **Tech backup for disaster recovery-** For any contingency, different locations will be identified from where the servers can be operated and backup mechanism for the data will be set in place. IT department has defined DC (Data Centre), DR (Disaster Recovery) policy to ensure continuous availability of critical customer centric services which aims towards mitigating the impact of disasters.

- **Defined infrastructure-**In the case of any disaster, backup preference wise location will be identified from where the operations could be handled and controlled. Bank will identify backup locations for critical business units to ensure uninterrupted customer service.

- **Restoration Plan-** Once the situation is well under control and is in stage of business as usual (BAU), the designated staff from various department viz. (Admin/IT/Security or Business owners) to ascertain that the situation has been perfectly restored. The Activities/transactions performed during BCP are to be maintained separately and to be shared with the stake holders for review and records.

5. Human Aspects of BCP

People are a vital component of any organisation. They should therefore be an integral part of a BCP. BCP awareness programme should also be implemented which serve to strengthen staff involvement in BCP. This can be done through induction programme newsletters, staff training exercises, etc.

HR consider cross-training employees for critical functions and document-operating procedures. Banks should consider possibility of enabling work-from-home capabilities and resources for employees performing critical functions.

6. Testing & Results

BCP for the respective units shall be subject to periodic “testing” (at least annually for all critical units, except for branches). This shall ensure that the formulated plans can be easily deployed, and Bank’s operations can be restored, within expected timeframes in the event of an actual contingency. Testing procedures and result shall be suitably recorded. Testing shall be conducted not only for all units in the bank but also for critical external support providers that render technology and non-technology support necessary to restore operations in the event of a disruption.

Various types of tests shall be carried out in the frequencies as pre-determined, and broadly the same should be classified as follows:

BCP testing for units: While conducting the tests, the respective units need to conduct at least two types of testing given below:

- ✓ **Site BCP Testing:** This scenario describes a contingency situation which deals with scenarios where the business site / premises may be rendered inaccessible or uninhabitable / unavailable due to fire, floods, local strike, power outage, systems not accessible etc. In such a case, units will be required to operate from alternate site location as identified in the BCP plan of critical units.

- ✓ **City BCP testing:** This scenario describes a contingency situation which deals with scenarios where the city is inaccessible due to act of terrorism, natural calamities of a severe magnitude etc. In such a case, units will be required to operate from an alternate city location as identified in the Unit’s BCP.

- ✓ **IT DR Testing:** IT Department shall conduct the DR Drill for critical applications of all business which have a DR set up. IT Department shall check whether the defined RTO (The acceptable amount of time to restore the service/application) and Recovery Point Objective -RPO (refers to the point in time in the past to which you will recover) are met and initiate suitable corrective measures if there is a gap.

- ✓ **Emergency Evacuation:** Admin & Security Departments shall be responsible for conducting Fire as well as Emergency evacuation drills at all offices / facilities and Branches of the bank.

  Learnings from the testing exercises or actual events shall be documented and shall be used for reviewing and improving future exercises thereby demonstrating continual improvement.

7. Review & Reporting

Review

- ➢ The Policy shall be reviewed at least annually or as necessitated due to material changes which may occur with premises, personnel, market, technology, or organizational structure. Any interim change(s) to the Policy shall be approved by the Chief Risk Officer (CRO) and the same shall be put up to board for approval subsequently.

- Internal Audit shall review the Business Continuity Plan documents of the units to ensure compliance with this policy.

Reporting

- An annual update describing the critical systems and BCP will be submitted to the respective Committee.
- A copy of the BCP, approved by the Board, should be forwarded for perusal to the RBI on an annual basis. In addition, the bank should also submit:
  – An annual statement at the end of each financial year describing the critical systems, their Rots and the bank's strategy to achieve them, and
  – A quarterly statement, reporting major failures during the period for critical systems, customer segment or services impacted due to the failures and steps taken to avoid such failures in future.

8. Training and awareness

AU Small Finance Bank will ensure that awareness and training programs, in accordance with Bank's Policy for participating teams are conducted to: -

- Communicate importance of the plan.
- Creating awareness about responsibilities and safety.