National Cooperative Bank, N. A.

Business Continuity Policy

Reviewing Board Committee	Audit Committee
Reviewing Management Committee	ORMC Committee
Responsible Executive	Cecil Greene/SVP, Chief Information Security Officer
Review Cycle	Annual (Second Quarter)
Last Approval Date	05/07/2020
Effective Date (if different)	

Business Continuity Policy

1. Purpose

It is the policy of National Cooperative Bank, N.A. ("NCB") and its affiliates as established by the institution's Board of Directors, to develop, implement, test and update annually the Business Continuity Management Program ("BCMP") in accordance with the Federal Financial Institutions Examination Council's Business Continuity Planning Booklet.

The purpose of this policy is to ensure the institution has business continuity plans in place to address all critical systems and operations if a situation occurs that adversely affects the normal daily operations of the institution.

2. Applicability

This policy applies to all NCB employees, contactors, and any other authorized users accessing data stores, information in any medium, and/or information systems. In addition, third parties may be subject to this policy through contractual obligations to NCB.

3. Definitions

Business Impact Analysis (BIA) – A document that identifies all critical IT systems/applications and prioritizes them based on criticality to NCB. The BIA is used to identify critical business functions and operations and the various IT assets needed to support them.

Computer Security Incident Response Team (CSIRT) – A formal project team, established in the Incident Response Plan (IRP), dedicated to incident response while handling events or incidents that may be impacting the confidentiality, integrity, or availability of the IT infrastructure, systems, applications, and data.

Disaster Recovery Plan (DRP) – A detailed set of instructions for recovering critical IT assets, systems, applications, and data to service the organization's mission critical business functions and operations in a prioritized manner.

4. Acronyms

BCP – Business Continuity Plan

BIA – Business Impact Analysis

CISO – Chief Information Security Officer (Designated BCP Coordinator)

CSIRT – Computer Security Incident Response Team

DRP – Disaster Recovery Plan

IRP – Incident Response Plan

ISSC – Information Security Steering Committee

IT – Information Technology

5. Policy

Each NCB Business Unit must maintain a Business Continuity Plan (BCP) that rolls up into an overall enterprise BCP. Business Unit Plans must include the following subsections:

For the enterprise level BCP, NCB will ensure the following:

- The BCP is written and implemented in accordance with the Federal Financial Institutions Examinations Council's Business Continuity Planning Booklet.

- NCB's DRP, a subset of the BCP, must define the recovery procedures necessary to restore critical IT assets during the outage.
- A formal Risk Assessment and BIA must be conducted in order to determine the requirements for the BCP. The Risk Assessment must be performed annually in order to address changes and updates to the BCP.
- The BCP will encompass critical business operations and functions primarily, and other non-critical business operations and functions secondarily.
- A formal backup and recovery plan must exist for all critical business operations and functions.
- Methods for responding to and recovering from cyber incidents, as detailed in the IRP, are referenced throughout the BCP.
- The BCP must be tested during three scheduled exercises a year to ensure that it can be implemented in emergency situations.
- The BCP must be kept up-to-date as changes are implemented to business operations and policies, and use of IT systems, applications, and data.
- All NCB employees are made aware of their roles, responsibilities, and accountabilities as it relates to the BCP.

6. Responsibility of Senior Management and Board of Directors

The Board of Directors is ultimately responsible for ensuring the existence of a Business Continuity Policy. It is the responsibility of management to ensure that a documented and tested Business Continuity Plan is developed that addresses all critical operations and functions of the bank. In this regard, the Board and Senior Management will:

1. Allocate sufficient resources and knowledgeable personnel to develop the Business Continuity Plan.
2. Set policy by determining how the institution will manage and control identified risks.
3. Review Business Continuity test results.
4. Approve the BCP on an annual basis.
5. Ensure the BCP is kept up-to-date and employees are trained and aware of their role in its implementation.

- The Chief Information Security Officer (Designated Plan Coordinator) shall be responsible for ensuring that management, though a BCP Committee or otherwise, oversee the review, implementation, and update of NCB's enterprise level BCP including the following steps: Update NCB's BCP annually, and present the BCP to the Board of Directors for review and approval.
- Oversee and approve the BCP annual testing.
- Monitor, participate (where possible), and review designated critical third party BCP testing.
- Oversee the annual update of the BIA.

- Oversee the annual Risk Assessment to identify all reasonable and foreseeable threats that could result in an outage situation. The results of the Risk Assessment must be provided to the Board of Directors annually to aid them in making an informed decision regarding the adequacy of NCB's BCP.

7. BCP Activation

Given any substantial interruption of service, whether caused by emergency, disaster or abnormal outage or downtime of critical IT systems, employees and contractors must be trained to inform the BCP Coordinator, who will follow the IRP and the BCP plan as appropriate. The BCP Coordinator will activate the BCP in order to restore normal business operations, functions, IT systems, applications, and data safely and as quickly as possible.

8. Notifications

In the event of an activation of the BCP, the Plan Coordinator will begin notification procedures by alerting the necessary CSIRT leaders first. The Plan Coordinator will also maintain contact information for local law enforcement and will determine if and when law enforcement is notified.

The Business Leaders and CSIRT leaders will utilize NCB's automated notification system during the emergency or disaster. It is important that all key personnel be notified of the emergency or disaster situation as soon as possible to begin business recovery operations. Internally, Business Unit managers are responsible for communication within their respective Business Units. Externally, the Marketing Department will represent NCB to the media should an event become publicly known.

9. BCP Testing

The enterprise BCP should be tested not less than three (3) times a year to ensure effective recovery preparedness. Managers from each business unit and the Business Continuity Team Leader will work with the BCP Coordinator to perform these Business Unit-Specific tests. All testing results are to be submitted to the BCP Coordinator promptly for evaluation. The BCP Coordinator will track all related BCP testing issues that are identified, and these issues will be presented to the ISSC Committee for resolution.

10. BCP Training

The BCP Coordinator will ensure that staff involved in BCP activities must be trained on business resumption and recovery by their respective Business Unit.

11. Exceptions

This policy is established for use within the NCB organization. If a Business Unit requires an exception from this policy a Policy, Standard and Procedure Request Form must be submitted clearly articulating the business reason for the exemption. Exemption requests will be reviewed by the BCP Coordinator and recommended to the ISSC for approval. Any exceptions to this policy shall be promptly reported to the Board at the next quarterly meeting unless circumstances warrant a shorter period of time.