CREDITACCESS GRAMEEN LIMITED

Business Continuity Policy

Version 1.5

Classification: *Internal use only*

Prepared by:	Saul Ruth S Ambat, Senior Manager – IT GRC
Reviewed by:	Ravi Rathinam, Chief Information Security Officer
Reviewed by:	Sudesh Puthran Chief Technology Officer
Reviewed by:	Gururaj Rao, Chief Audit Officer
Recommended by:	Udaya Kumar, Managing Director

Contents

Revision History

Rev. No.	Author	Date of Approval	Reason for Change
1.0	Arun Kumar B	01/09/2017	First Release
1.1	Arun Kumar B	14/10/2019	Inclusion of COO & CRO as signatory
1.2	Mansoor Ahmed T K	25/10/2021	Policy review and update
1.3	Mahantesh Dhangi	21/10/2022	Policy review and Inclusion of CISO as signatory
1.4	Ravi Rathinam, Chief Information Security Officer	21/07/2023	Annual Review and included requirements from RBI Circular & ISO 22301. • BC Plan to be tested for various scenarios' • Business Continuity Policy section amended to mandate BC testing, defined DR drill periodicity for critical systems as 6 months and non-critical system as annual • Documentation of recovery strategies, backup & restoration requirements, reconciliation for non-zero RPO after DR drill, and to have system configurations and patch levels in DR to be the same as primary DC.

			• External & Internal Communications • DR testing for the new applications
1.5	Saul Ruth S Ambat	April 1, 2024	Inserted Section 6 to cover BCP and DR of interconnected systems, as required under latest RBI Guidelines on GRC dated Nov 7 2023.

Purpose

The purpose of this document is to define the policy to ensure continuity, resumption, and recovery of critical business processes in the event of disruptions.

Abbreviations

Abbreviation	Meaning
IT	Information Technology
IS	Information Systems
CAGL	CreditAccess Grameen Limited
BCP	Business Continuity Plan
DR	Disaster Recovery
BIA	Business Impact Analysis (BIA)
CAAT	Computer Assisted Audit Techniques
RBI	Reserve Bank of India
NBFC	Non-Banking Financial Company
MFI	Micro Finance Institution
BIA	Business Impact Analysis
RTO	Recovery Time Objectives
RPO	Recovery Point Objectives
CTO/CIO	Chief Technology/Information Officer
MTPD	Maximum Tolerable Period of Disruption

Business Continuity Policy

1. Business Continuity Plans (BCP) /Disaster Recovery plans (DRP) shall be developed based on a Business Impact analysis (BIA).
2. BIA shall be conducted/reviewed at least once annually.
3. Recovery time objectives (RTO) and Recovery Point Objectives (RPO) will be identified and considered when establishing the business continuity plans and disaster recovery plans.
4. BC Plan shall be regularly tested under different scenarios for all possible types of contingencies, to ensure that it is up-to-date and effective. Testing of BCP shall include all relevant aspects and constituents i.e. People, Processes and Resources (including Technology).

5. Periodicity of DR drills for critical information systems shall be at least on a half-yearly basis and for all other systems at least on a yearly basis. Any major issues observed during the drill shall be resolved and tested again, to ensure successful conduct of drill before the next cycle. The DR testing shall involve switching over to the DR/ alternate site and thus using it as the primary site for sufficiently longer period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.
6. In case of critical interconnected systems, the BCP and DR will be documented and performed in such a way to ensure collective readiness to meet the RTO.
7. Shall document recovery strategies / details of the actions that the teams will take in order to continue or recover prioritized activities within predetermined timeframes and to monitor the effects of the disruption and the organization's response to it.
8. Shall document on communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate.
9. BCP/DR plans shall be updated/revised based on the outcomes of the tests where required.
10. BCP/DR plans shall be reviewed annually and updated when significant changes are made to the business processes or the underlying IT infrastructure and application ecosystem.
11. BCP/DR shall be considered in all new projects/new initiatives.
12. DR shall be tested for all new applications / infrastructure before deployed in production
13. Shall Backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorised access.
14. In a scenario of non-zero RPO, CAGL shall have a documented methodology for reconciliation of data, while resuming operations from the alternate location.
15. Shall ensure that the configurations of servers, network devices, other products and deployed security patches at the DC and DR are identical.
16. Relevant personnel shall be trained on business continuity and disaster recovery plans and informed about their roles and responsibilities.
17. Documentation of the BCP/DR plans shall be maintained (including off site as necessary) to ensure it is accessible when the business continuity plan or the disaster recovery plan has to be invoked.
18. BCP/DR plans shall also consider vendors/suppliers/third parties as part of establishing, documenting, evaluation/testing and maintaining the BCP/DR plans.

Documented operating procedures

1. Documented operating procedures shall be established to implement the requirements of this policy.
2. The implemented documented operating procedures shall be reviewed and updated at least once annually.

Implementation

1. This board approved policy shall be implemented with the organization by relevant teams and departments.
2. Compliance to this policy and implementation status shall be evaluated at least annually in keeping with assurance requirements indicated above and reported to the board.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action as defined in the procedure for Disciplinary Action, up to and including termination of employment. A violation of this policy by a temporary employee, contractor or vendor may result in the termination of their contract or assignment with CA Grameen.

Exceptions to this Policy

All exceptions to this policy shall be explicitly approved by the CTO. The exception shall be valid for a specific period and shall be reassessed and re-approved when necessary.