CREDITACCESS GRAMEEN LIMITED

Business Continuity Policy

Version 1.7

Classification: *Internal use only*

Revision History

Version	Author	Description of Changes	Release Date
1.0	Arun Kumar B	First Draft	04/10/2017
1.1	Arun Kumar B	Inclusion of COO & CRO as signatory	30/10/2019
1.2	Mansoor Ahmed T K	Policy review and update	09/11/2021
1.3	Mahantesh Dhangi	Policy review and Inclusion of CISO as signatory	21/10/2022
1.4	Ravi Rathinam, Chief Information Security Officer	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	21/07/2023
1.5	Saul Ruth S Ambat	Inserted Section 6 to cover BCP and DR of interconnected systems, as required under latest RBI Guidelines on GRC dated Nov 7, 2023.	April 1, 2024
1.5	Saul Ruth S Ambat	Re-adoption	Mar'25
1.6	Shruthi Laxmain	Exceptions to Policy: removed Section 3.1: Updated for Head office personnel unavailability. Section 4 : Updated for BCP	April 16, 2026

Version Control

Version	Author	Reviewed by	Approved By
1.0	Arun Kumar B	Gururaj Rao - Head – Risk Management Udaya Kumar - Managing Director & CEO	IT Strategy Committee
1.1	Arun Kumar B	R Venkatesh Prasad - Chief Operating Officer Anshul Sharan - Chief Risk Officer Gururaj Rao - Chief Audit Officer Udaya Kumar - Managing Director & CEO	Board of Directors
1.2	Mansoor Ahmed T K	Sudesh Puthran - Chief Technology Officer Gururaj Rao - Chief Audit Officer Mahadev Prakash - Head – Compliance, Legal & Company Secretary Udaya Kumar - Managing Director & Chief Executive Officer	Board of Directors
1.3	Mahantesh Dhangi	Ravi Rathinam - VP-Information Technology & Chief Information Security Officer Sudesh Puthran - Chief Technology Officer Gururaj Rao - Chief Audit Officer Udaya Kumar Hebbar - Managing Director & CEO	Board of Directors
1.4	Ravi Rathinam, Chief Information Security Officer	Sudesh Puthran - Chief Technology Officer Gururaj Rao - Chief Audit Officer Udaya Kumar Hebbar - Managing Director & CEO	Board of Directors
1.5	Saul Ruth S Ambat	Ravi Rathinam - Chief Information Security Officer Sudesh Puthran - Chief Technology Officer Firoz Anam – Chief Risk Officer Gururaj Rao – Chief Operating Officer Udaya Kumar Hebbar – Managing Director & CEO	Board of Directors
1.5	Saul Ruth S Ambat	Ravi Rathinam - Chief Information Security Officer Sudesh Puthran - Chief Technology Officer Firoz Anam – Chief Risk Officer Gururaj Rao – Chief Operating Officer Udaya Kumar Hebbar – Managing Director & CEO	Board of Directors
1.6	Shruthi Laxmain	Ravi Rathinam - Chief Information Security Officer Sudesh Puthran - Chief Technology Officer Firoz Anam – Chief Risk Officer Gururaj Rao – Chief Operating Officer Ganesh Narayanan - MD & CEO	Board of Directors

CONTENTS

Business Continuity Policy

1. 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	Credit Access 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

2. Introduction

Business Continuity Plan (BCP) refers to a detailed document outlining how an organization will continue to operate during and after a disruptive event. It identifies critical business functions, processes, and systems that need to be sustained or restored, and details the procedures for maintaining them. Essentially, a BCP acts as a strategic playbook for ensuring business stability and minimizing disruption in the face of various threats, such as natural disasters, cyberattacks, or other unforeseen circumstances.

The BCP shall contain following elements

- **Threat / Nature of Disruption**

  The external factor causing disruption

- **Risk Assessment:**

This involves identifying potential threats and vulnerabilities to the business, as well as assessing the likelihood and potential impact of each threat.

- **Recovery Strategies:**

  This outlines the steps and procedures for restoring business operations and critical systems after a disruption.

- **Communication Plan:**

  This defines how the organization will communicate with stakeholders (employees, customers, partners) during and after a disruption.

- **Testing and Maintenance:**
  Regular testing and updates of the BCP are crucial to ensure its effectiveness and relevance in a changing business environment.

3. Scope

The business continuity plan shall cover key business processes of the company such as loan processing & disbursal and collection. Given that external threats requiring BCP are localized in nature , the plan must be specific to the operational centers. Accordingly, separate plan for Branch, Regional Processing Center (RPC) / Regional Office and HO has been provided.

The BCP for IT systems involve activating the Disaster Recovery (DR) in case of low availability. The details has been spelt out in a separate section.

4. BCP for operational locations

4.1 BCP for Head Office, Bangalore

Nature of Disruption	Risk Assessment	Recovery Time Objective	Recovery Strategy, Resource Dependency & Communication	Responsibility
Civil Disturbances like Mass Protest, Riot, Bandh etc.	Employees can't reach the office, leading to work disruption. Physical damage to premises Employee Safety	Immediate	Employees to be contacted through emails / mobile phones and asked to work from home. In case of sudden disturbances	MD/CEO will take decision supported by Head (Admin) and issue communication with help from Head - HR

			during working hours, entry/exit will be restricted till situation normalizes The company has moved to a laptop first model for most employees in support functions. The list of employees with laptops can be increased on a need basis. Employees requiring critical system access to have VPN access.	
Natural disaster like Flood, Cyclone, Earthquake	Employees can't reach the office. Physical damage to premises	Immediate	Employees to be contacted through email/mobile phone and asked to work from home. as soon as warning is received. All employees are issued Laptop. Employees requiring critical system access to have VPN access. If warning received during working hours, employee may be asked to leave office depending	

			on the expected time of occurrence	
Fire	Employee Safety	Immediate	Head-Admin to initiate fire safety protocol immediately Employees to be asked to work from home as soon as warning is received. All employees are issued Laptop. Employees requiring critical system access to have VPN access.	
Pandemic	Employee Safety	Immediate	Employees will be asked to work from home as soon as the warning is received. All employees will be issued Laptops. HODs shall have a system of tracking affected employees and transfer work to back-up resources when required. Employees requiring critical system access to have VPN access.	

Internet Shutdown	Disruption in regular operation It will not be possible to support and monitor branch operations from HO	24 hours	Communication between HO and RPC / Branch to be conducted through phone (voice & sms) instead of email If persists beyond 48 hours, a group of selected staff can be sent to nearby town / city where Internet is available	MD/CEO will take decision supported by Head (Admin) and issue communication with help from Head - HR
Sudden Loss of Key Personnel in support functions	Disruption in regular activities such as IT/Finance/regulatory reporting/ Risk etc	Immediate	HOD will arrange alternate resource The HoD shall maintain a list (where applicable) of external vendors from where resource could be procured on short notice HoD may also identify alternate resource within or outside department The organization shall implement workforce continuity measures, including but not limited to cross-training of critical personnel, designation of role backups, and formal succession planning, to ensure operational resilience and	HOD shall decide to invoke BCP

			mitigate risks arising from staff unavailability.	
Cyber incidents / IT incidents leading to unavailability of systems	-		Refer Annexure 2	

4.2 BCP for Regional Office / RPC

Nature of Disruption	Risk Assessment	Recovery Time Objective	Action To be Taken & Resource Dependency	Responsibility
Civil Disturbances like Mass Protest, Riot, Bandh etc.	Employees can't reach the office. Physical damage to premises Employee Safety	Immediate	Employees to be contacted through email/mobile phone and asked to work from home. In case of sudden disturbances during working hours, entry/exit will be restricted till situation normalizes All employees to be issued Laptop. Employees requiring critical system access to have VPN access.	Zonal/Regional Manager, to co- ordinate all action steps and communicate to HO, Branches and other stakeholders
Natural disaster like Flood, Cyclone, Earthquake	Employees can't reach the office. Physical damage to premises	Immediate	Employees to be contacted through email/mobile phone and asked to work from home as soon as warning is received. All employees are issued Laptop. Employees requiring critical system access to have VPN access.	

			If warning received during working hours, employee may be asked to leave office depending on the expected time of occurrence	
Fire	Employee Safety	Immediate	Employees will be sent to home/ asked to work from home. Selected employees will be issued Laptops. Workload can be transferred to other RPCs if there is prolonged disruption.	
Pandemic	Employee Safety	Immediate	Employees will be asked to work from home as soon as the health warning is received. Selected employees will be issued Laptops. Additional laptops needed to be arranged so that all employees can work from home	
Internet Shutdown	Disruption in regular operation Centralized operations activity will be disrupted It will not be possible to support and monitor branch operations	24 hours	Communication between Regional Office/RPC and HO / Branch to be conducted through phone (voice & sms) instead of email Work can shifted to nearby RPCs If persists beyond 48 hours, a group of selected staff can be sent to nearby town / city where Internet is available	
Cyber incidents / IT	-		Refer Annexure 2	

incidents leading to unavailability of systems				

4.3 BCP for Branches

Nature of Disruption	Risk Assessment	Recovery Time Objective	Action To be Taken & Resource Dependency	Responsibility
Civil Disturbances like Mass Protest, Riot, Bandh etc.	Collection activity will get impacted resulting in high delinquency. Loan disbursal will stop, leading to loss of business	24 Hours	Kendra Leader to be contacted by phone. Contact individual customers by phone wherever necessary. Collection day can be shifted if Kendra location is impacted. Collection through online mode (UPI) wherever possible. Loan disbursal can be deferred.	BM/ABM to communicate the branch staff for initiation of BCP. Will invoke BCP in discussion with AM/DM/ZM
Natural disaster like Flood, Cyclone, Earthquake	Collection activity will get impacted resulting in high delinquency. Loan disbursal will stop, leading to loss of business	72 Hours	Kendra Leader to be contacted by phone. Contact individual customers by phone where necessary. Collection day can be shifted if Kendra is impacted. Collection through online mode (UPI) wherever possible. Loan disbursal can be deferred to future dates while informing the customer. If employees are impacted, additional staff from nearby branches or BST/Audit/Risk staff can be deployed.	

Fire	Employee Safety	Immediate	Loan disbursal can be deferred. If employees are impacted, additional staff from nearby branches or BST/Audit/Risk staff can be deployed.	
Pandemic	Employee Safety	Immediate	Kendra Leader to be contacted by phone. Contact individual customers by phone where necessary. Collection day can be shifted if Kendra is impacted. Collection through online mode (UPI) wherever possible. Loan disbursal can be deferred to future dates while informing the customer. If employees are impacted, additional staff from nearby branches or BST/Audit/Risk staff can be deployed	
Internet Shutdown	Disruption in regular operation loan such as loan processing & collection	24 hours	Communication between Regional Office/RPC/HO and Branch to be conducted through phone (voice & sms) instead of email Cash collection to be kept in the vault if bank branches are not open If persists beyond 48 hours, a group of selected staff can be sent to nearby branch where Internet is available	BM/ABM to communicate the branch staff for initiation of BCP. Will invoke BCP in discussion with AM/DM/ZM
Cyber Attack / IT incidents	-		Refer Annexure	

leading to unavailability of systems				

4.4 Periodic Testing

The plan (BCP) shall be tested periodically (preferably once in a year) simulating one or multiple threat / disruption types
Documentation of the BCP 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.

5. Business Continuity for IT Resources

BCP for IT resources is achieved through invoking DR(Disaster Recovery). The Salient feature of DR is outlined below:

a) For every critical IT system there will be DR plan which is developed based on a Business Impact analysis (BIA).
b) BIA shall be conducted/reviewed at least once annually.
c) Recovery time objectives (RTO) and Recovery Point Objectives (RPO) will be identified and considered when establishing the business continuity plans and disaster recovery plans.
d) DR 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 DR shall include all relevant aspects and constituents i.e. People, Processes and Resources (including Technology).
e) Periodicity of DR drills for critical 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.
f) In case of critical interconnected systems, the DR will be documented and performed in such a way to ensure collective readiness to meet the RTO.
g) 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.
h) Shall document on communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate.

i) BCP/DR plans shall be updated/revised based on the outcomes of the tests where required.
j) 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.
k) BCP/DR shall be considered in all new projects/new initiatives.
l) 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.
m) In a scenario of non-zero RPO, CAGL shall have a documented methodology for reconciliation of data, while resuming operations from the alternate location.
n) Shall ensure that the configurations of servers, network devices, other products and deployed security patches at the DC and DR are identical.
o) Relevant personnel shall be trained on business continuity and disaster recovery plans and informed about their roles and responsibilities.
p) 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.
q) BCP/DR plans shall also consider vendors/suppliers/third parties as part of establishing, documenting, evaluation/testing and maintaining the BCP/DR plans.
r) The organization shall formally assess and document all dependency risks between the primary site and the disaster recovery (DR) site, including but not limited to shared infrastructure components, network connectivity, authentication mechanisms, third-party services, and any common points of failure that could adversely impact the effectiveness of disaster recovery operations.

6. Business continuity in case of Unavailability of DR

Extent of Impact / Availability	Action to be Taken	Responsibility
No critical system is impacted	All activities shall be postponed till the system is available.	COO to ensure communication to all branches and RPC
Critical System Impacted – Infor	All payments shall be postponed till the system is available. Other transaction details from CBS shall be collected and maintained in Excel and further processed manually.	CFO for communication and implementation of the process
Critical System Impacted – T24	Loan applications can be processed through Maitri for one week and disbursement can be processed manually through cash at field for Loans <=20K.	COO for communication and

	Loans which are >20K shall be processed through manual NEFT. Collection sheet can be downloaded for a period of one week from BRP and collections to be made manually by the field. Records to be maintained by field team properly. Post the initial week, all activities shall be postponed till the system is available. Bank deposit slips shall be collected manually through email to the accounts team or hard copy can be kept in the branch.	implementation of the process
Critical System Impacted – Maitri/DigiAgil	Paper application to be collected by KM. Branch shall send the day's collected application to CRT in a pre-defined excel format. CB report shall be fetched through PR. All policy parameters shall be checked by the Risk Analytics team and decision provided in each application. The Processing fees and insurance interest will be calculated with the help of Risk Analytics team with a pre-approved script and provided to CRT team for further processing. The disbursement shall be initiated in T24 through CRT file uploads post getting the details of the loan from branches and the details of the charges & decisions (CB Results) from Risk team. Passbooks and KFS shall be generated directly from CBS (T24). New customer onboarding shall be put on hold till such time DigiAgil is up. Static data updates for the existing customers will also be put on hold. Collections will be directly posted in T24.	COO for communication and implementation of the process
Critical System Impacted – BRE	Applications data shall be downloaded from Maitri/DigiAgil. CB report shall be fetched through PR. All policy parameters shall be checked by the Risk Analytics team through predefined scripts and decision is provided to each application(s). The file shall be passed on to the CRT team for manual upload to Maitri for sanction and disbursal. CRT team can be temporarily provided with additional resources from different teams to support volumes.	COO for communication and implementation of the process

	The Processing fees and insurance interest will be calculated with the help of Risk Analytics team with a pre-approved script and provided to CRT team for further processing.	
Critical System Impacted – Mahi	All activities shall be postponed till the system is available. Customer can approach the nearest branches for any financial requirements/ Clarifications/Repayments. This is possible as Mahi is being implemented only in a certain radius from existing branches. Customers can also call our member care nos. basis which KM's would also be deployed for cash collections from digital customers. An SMS to be sent to all Mahi customers informing them about the disruption of Mahi services and with contact information for their immediate requirements, if any. Field teams to be proactively informed about the outage to ensure they address customer queries if any at ground.	COO for communication and implementation of the process
Critical System Impacted – NewGen / Amoga	**Unnati and Two-Wheeler loans:** Loan data entry can be done manually or through a survey form, reviewed by a central team. Eligibility can be done through a manual PR pull. PD data can further be added to the same survey form. Basis PD data, central team can calculate the eligible loan amount. For all eligible cases, sanction documents to be generated manually and loan entry is also carried out manually in T24. Final approval done from the branch in T24 and disbursement documents again can be manually generated and shared to branches. **For Mortgage loans:** Loan data entry can be done manually or through a survey form, reviewed by a central team. Eligibility can be done through a manual PR pull. For all eligible cases, credit team can do the eligibility calculation through the excel template available. Legal and technical will be manually triggered as it is done today. All deviations will be manually managed by the credit team with all approvals on	COO for communication and implementation of the process

	email. Basis all criteria met, central ops can create loan in T24, which then get sanctioned by the branch team. All the documents to be generated manually. Signed disbursement documents to be shared to central operations via email for final approval for disbursement from the branch through T24.	
Email is not available	If both the email platforms are not available, communication can be done through other approved messaging platforms. If only one email exchange server is impacted, the services will be moved to the other exchange server	CTO to send communication
More than one critical system including T24 & Maitri is impacted	Manual system of loan application (in paper form) to be initiated. Loan application to be sent to RPC (scanned and emailed). RPC will verify the loan application (approved by appropriate DoP) along with KYC detail. RPC shall prepare the list of application in a specific excel format and send to CRT. CRT shall initiate CB check through PR with support from risk analytics function. CRT shall prepare a list of sanctioned loan and sent to respective branches to complete the disbursal formalities. Upon confirmation from branch, CRT shall send the list to central ops for disbursal. Collection to be recorded in paper notebook at customer level. Bank deposit slip to be sent to HO via email along with copy of the notebook.	COO for communication and implementation of the process

7. 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.

8. 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.

9. 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.