CREDITACCESS GRAMEEN LIMITED

Cyber Security Policy

Revision History

Version	Author	Description of Changes	Release Date
1.0	Arun Kumar B	First version	September 01, 2017
1.1	Arun Kumar B	Modified version for Board Approval	September 29, 2017
1.2	Arun Kumar B	Inclusion of COO & CRO as signatory	October 14, 2019
1.3	Mansoor Ahmed T K	Policy review and update	October 25, 2021
2	Arun Kumar B	Amendments to clauses - Training & Awareness, Penetration Testing, Cyber Security Operations Centre, Patch Management and Cyber Crisis Management Plan	March 23, 2022

Version	Author	Reviewed by	Approved by
1.0	Arun Kumar B	MD & CEO	Board of Directors
1.1	Arun Kumar B	MD & CEO	Board of Directors
1.2	Arun Kumar B	MD & CEO	Board of Directors
1.3	Mansoor Ahmed T K	MD & CEO	Board of Directors
2	Arun Kumar B	MD & CEO and CTO	Board of Directors

Contents

1. Purpose:

Cyber security shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalized telecommunications network, and to the set of objects themselves where they present interfacesallowing their remote control, remote access to data, or their participation in control actions withinthat cyberspace. Cyberspace is a complex environment consisting of interactions between people,software and services supported by worldwide distribution of information and communication technology, devices and networks.

Cyber security is defined by The Oxford English Dictionary as "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". In reality, cyber security has come to encompass domains such as communications security, operations security, physical security within the overall purview of information security and broadly refers to all security aspects relevant to the 'digital world' today often focusing on the basic tenets of confidentiality, integrity, availability, and authenticity. The Joint technical committee ISO/IEC JTC1/SC27 IT-Security Techniques, in the document ISO/IEC 27032:2012 - Information technology—Security techniques—Guidelines for cybersecurity defines cyber security as the preservation of confidentiality, integrity and availability of information in the cyberspace which in its broadest sense is suitable for the purposes here and also intermeshes with the overallinformation security initiatives in the organization which are focused on the protection of the confidentiality, integrity and availability of all information in the organization irrespective of its presence in cyberspace or outside.

Further for the purposes of this document and for effective definition of the cyber security policyin CA Grameen, reference is also made to the definition of cyber security as provided by International Telecommunication Union (ITU), which defines cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets.

Considering the extensive use of digital technology/cyber technology, it has become imperative for CA Grameen to put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.

The purpose of this document is to define a cyber security policy considering the information security policy, which would provide management direction and support for cyber and information security in accordance with business requirements and relevant laws and regulations of the country.

The following fundamental principles will also contribute to cyber security policy and further implementation of the necessary cyber security related controls:

a) Recognition of the strategic importance of cyber security.
b) Importance of assigning responsibility for cyber security to ensure effective implementation of necessary measures for cyber security.
c) Establishing appropriate governance model for cyber security.
d) Fostering a risk-based approach to cyber security so as to ensure needs of all

stakeholders are met.

e) Ensuring appropriate mechanisms to detect, respond, recover and contain cyber security incidents.

f) Continual reassessment of cyber security profile of the organization so that necessary corrective and preventive actions can be initiated as required.

Note:

1. The following usages of cyber security and cybersecurity within this document and acrossother documentation within the organization are intended to mean the same.
2. Cyber and digital are used to mean the same and encompass resources, information data and all allied resources which support the organization's computer/digital /cyber activities.

2. Abbreviations:

Abbreviation	Meaning
IT	Information Technology
IS	Information Systems
RBI	Reserve Bank of India
NBFC	Non-Banking Financial Company
MFI	Micro Finance Institution
ISO	International Organization for Standardization
ITU	International Telecommunication Union
IEC	International Electrochemical Commission
JTC	Joint Technical Committee
BCP	Business Continuity Plan
DRP	Disaster Recovery Planning
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

3. Cyber security policy:

In keeping with the cyber security needs of CA Grameen, the following policy statements are adopted to provide guidance to the cyber security initiatives in the organization. It should also beensured that necessary governance framework, organization structures with competent staff resources, resources for design and implementing cyber security controls, monitoring, assessment and improvement is carried out on an ongoing basis.

4. Policy Statements:

A. Information access control:

A.1 Access to information especially digital information will be controlled and provided based on an assessment of the requirements for confidentiality, integrity, authenticity and availability of such information.

B. New technology adoption:

B.1 New technology adoption will be driven by a clear understanding of the need for such technology and evaluating the fit of such technology in line with the overall IT strategy established by CA Grameen. Consideration shall also be given to the cyber risks from

suchtechnology and the ability to appropriately mitigate such risks.

B.2 All new technology adoption shall be reviewed and presented to the management and / Board.

C. Network protection:

C.1 The network is the key element of cyber space and suitable protection shall be ensured forall the network elements for cyber security. Suitable technologies and technology solutionsincluding but not limited to firewalls, end-point protection, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) etc. will be used to secure the network. Appropriate monitoring of network and network security shall be carried out.

D. Risk assessment:

D.1 Cyber security risk assessment shall be carried out in conjunction with IT risk assessmentto ensure that relevant threats are identified, and controls implemented for mitigation.
D.2 Status of identified cyber security risks shall be monitored on an on-going basis andappropriate adjustments carried out to ensure that risk assessment is current.
D.3 Status of identified mitigation actions shall be tracked to closure and reported to themanagement.

E. Hardening:

E.1 All elements of the cyber landscape shall be hardened as per applicable standards / bestpractices or recommendations from vendors.
E.2 Baselines shall be established for hardening of elements of the cyber landscape such asservers, routers, switches etc.

F. Back-up & restoration testing:

F.1 Back-ups of data / information shall be taken as per established policy and procedures.
F.2 Restoration shall be carried out and records maintained.
F.3 Back-ups shall be retained as per defined policy and procedures and accessibility to back-ups shall be ensured at all times.

G. Access to computing resources:

G.1 Access to computing / cyber resources shall be provided on a need basis.
G.2 Rights shall be assigned considering the need for segregation of duties and to preventfraud, collusion etc.
G.3 Access rights shall be reviewed once every six months and revoked / removed in case foundin excess of need.
G.4 Access rights shall be removed at the time of exit / transfer or change in role.

H. Management of outsourced activities:

H.1 Outsourcing activities carried out relating to cyber/digital resources used by CA Grameen shall be based on appropriate due diligence and evaluation of the need to outsource in linewith the organization strategy and consideration of risks from any contractual arrangementsand regulatory compliance obligations.

H.2 Outsourced activities shall be managed as per established policies and procedures.
H.3 Outsourced activities shall be monitored and right to audit by the organization and its stakeholders including statutory and regulatory agencies shall be ensured contractually.

I. Training/awareness:

I.1 Training and awareness shall be planned and provided to relevant personnel to ensurecyber security.
I.2 Competency requirements for personnel shall be identified relating to cyber security andshall be ensured at all times.
I.3 Effectiveness of cyber security training and awareness measures shall be evaluated, andnecessary actions taken.
I.4 Evidence to demonstrate the delivery of training / awareness relating to cyber security shallbe retained.
I.5 Timely completion of trainings on Information security awareness may be made part of employee performance evaluation process.

J. Communication technology:

J.1 Communication technology forming or supporting cyber activities in the organization shall be governed keeping in consideration risks and relevant regulatory compliance obligations.

K. Vulnerability management:

K.1 Vulnerabilities relating to the digital / cyber infrastructure shall be managed to prevent /mitigate cyber risks and incidents by carrying out periodic vulnerability assessments
K.2 Vulnerability assessments shall be carried out at least on an annual basis.
K.3 Vulnerabilities shall be identified based on an established vulnerability management strategy.
K.4 Action plans shall be defined to remedy identified vulnerabilities and tracked to closure.
K.5 Status of vulnerability management activities shall be monitored and reported to concernedlevel of management.

L. Penetration Testing

L.1 Penetration testing in all the critical internet facing applications shall be undertaken on a periodic basis, once in a year.
L.2 L.2The testing activity is preferred to be outsourced to a competent Third-Party Service Provider.

M. Cyber Security Operations Centre (SOC)

M.1 Cyber SoC covering critical applications, shall be put in place taking into account, proactive monitoring and management capabilities with sophisticated tools for detection, response, backed by data for sound analytics.

M.2 InfoSec team is responsible for reviewing the SOC alerts on a daily basis and the outcome of the SOC exercise shall be presented to the Senior Management at an appropriate frequency.

N. Patch Management

N.1 To follow a documented process for inventorying IT components that need to be

patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

O. Assurance framework shall be established:

O.1 A cyber security assurance / audit framework shall be established where all cyber securityactivities shall be audited at least once a year.
O.2 Audit findings shall be acted upon and reported to the management and reported to theBoard / Board Committees as the case may be.
O.3 Appropriate changes shall be made to the cyber security related activities in the organization in keeping with the findings/outcomes of the cyber security assurance/audit.

P. Business continuity planning (BCP) / Disaster recover planning (DRP):

P.1 Planning to ensure continuity of business post cyber security events / incidents shall becarried out and implemented.
P.2 A BCP / DRP shall be implemented based on business impact analysis.
P.3 Plans established, as part of the BCP/ DRP shall be tested periodically/ at least annually asper plans.
P.4 Actions shall be taken based on the outcomes of the testing including updates to the BCP /DRP.
P.5 Status of the BCP / DRP activities shall be reported to relevant levels of management and the Board.

Q. Resilience:

Q.1 Resilience of cyber infrastructure shall be planned and implemented.
Q.2 Capability of infrastructure to meet resilience requirements on an on-going basis shall beevaluated and tested periodically and necessary actions taken.
Q.3 Resiliency requirements shall be considered when new cyber infrastructure is being established and shall be implemented accordingly.

R. Cyber security preparedness indicators:

R.1 Cyber security preparedness shall be monitored proactively by establishing metrics.
R.2 Early warning indicators shall be identified and monitored to ensure cyber security preparedness.
R.3 Cyber security preparedness indicators shall be used for comprehensive testing throughindependent compliance checks and audits / for assurance programs.

S. Cyber crisis management plan:

S.1 A cyber crisis management plan shall be established addressing detection, response,recovery, and containment.
S.2 Cyber crisis management plan shall consider scenarios identified based on a business impactanalysis.
S.3 Appropriate corrective and preventive actions shall be initiated based on the identified cybercrisis scenarios.
S.4 Cyber crisis management plan shall be evaluated at least on an annual basis and updated as required.
S.5 Declaring 'Cyber Crisis' and escalating to 'Cyber Crisis Management Team (CCMT)'

- Upon the knowledge of the problem from any source, the Chief Technology Officer (CTO) and Information Security Officer / Team would assess the situation and after due urgent discussion with senior management. CTO will decide whether 'Cyber Crisis' needs to be declared.
- If the systems are required to be shut down including e-mail, then the time of verbal declaration would be noted down and should be appropriately notified via email upon its functioning.
- All the members of the Cyber Crisis Management Team (CCMT) will be advised over telephone about such declaration. The members of CCMT will spring into action immediately. Security Crisis may be declared based on the following incident and above parameters.
- CCMT call tree matrix:

No	Designation
1.	Chief Technology Officer
2.	Head - IT Application - GL
3.	Head - IT Application - RF
4.	Head – IT Infrastructure
5.	Chief Information Security Officer
6.	Chief Risk Officer
7.	Chief Compliance Officer

- Roles and Responsibilities of CCMT:

Role	Responsibilities
Chief Technology Officer (CTO)	• To coordinate with Business Heads and advise them on the situation • Coordinates the IT implementation efforts with the technology team within the CA Grameen and with the third parties who are maintaining or managing the IT infrastructure
Chief Information Security Officer (CISO)	• Coordinates the security controls evaluation and implementation efforts with the Information Security Team within the CA Grameen and with the IBM/CtrlS who are maintaining or managing the IT infrastructure • To coordinate with Business Heads and advise them on the situation
Head - IT Application	• Engage with his team for isolating systems affected / • restoring backups if necessary and all other systems and application related operational issues
Head - IT Infrastructure	• Engage with his team for isolating systems affected / • restoring backups if necessary and all other infrastructure and application related operational issues
Chief Risk Officer (CRO)	• CRO will be directly involved for the Risk Assessment phases and give guidance to the CCMT during the crisis management
Chief Compliance Officer	• Provide consultation on the legal standing of the CA Grameen during the Cyber security crisis situation • Provide legal support during the litigation or lawsuit • Coordinate with regulators and provide update on crisis
Respective	• Continuously work with their respective teams to address

Business Heads	the concerns and issues of the branch staff and customers

T. Cyber security incident analysis and monitoring:

T.1 Cyber security incidents shall be identified, recorded, monitored, and analyzed.
T.2 Actions including corrective and preventive actions shall be taken on cyber securityincidents.
T.3 Cyber security incidents shall be reported as applicable to the relevant regulatory authorities.
T.4 CA Grameen shall conduct root-cause analysis (RCA) for critical severity incident to ensure adequate response and support recovery activities are clearly identified.

U. Documented operating procedures:

U.1 Documented operating procedures shall be established to implement the requirements ofthis policy.
U.2 The implemented documented operating procedures shall be reviewed and updated at leastonce annually or as and when changes are made to the requirements based on
U.3 Risk assessments
U.4 New additions or changes in IT/IS systems in the organization
U.5 Cyber security incidents
U.6 Changes in statutory and regulatory requirements etc.

5. Implementation:

1. This Board approved Cyber Security Policy shall be implemented within CA Grameen byrelevant 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.

6. 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.

7. Exceptions to this Policy:

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

****