REGULATION Nº 02/2018 OF 24/01/2018 ON CYBERSECURITY

TABLE OF CONTENTS

REGULATION Nº 02/2018 OF 24/01/2018 ON CYBERSECURITY

Pursuant to Law n° 48/2017 of 23/09/2017governing the National Bank of Rwanda, especially in Articles 6, 8, 9 and 10;

Pursuant to Law n° 47/2017 of 23/094/2017 governing the organization of banking especially in its Article 37 and 117 ;

The National Bank of Rwanda hereinafter referred to as "Central Bank", decrees:

CHAPTER ONE: GENERAL PROVISIONS

Article one: Purpose

This regulation aims at :

1° establishing minimum prudential standards to banks for their protection against cybersecurity threats ; and

2° promoting the protection of customer information as well as the information technology systems of banks

Article 2: Definition of terms

In this regulation, the following words and expressions shall mean:

1° **affiliate**: any person that controls, is controlled by or is under common control with another Person. In this definition , control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise ;

2° **authorized User**: any employee, contractor, agent or other person that participates in the business operations of a bank and is authorized to access and use any Information Systems and data of the bank ;

3° **cybersecurity incident**: any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

4° **information System**: a discrete set o electronic information resource organized for the collection, processing maintenance, use, sharing dissemination or disposition o electronic information, as well as any specialized system such as industrial/process controls systems telephone switching and private branch exchange systems, and environmenta control systems.

5° **multi-Factor authentication** authentication through verification of a least two of the following types o authentication factors:

a) knowledge factors, such as a password;
b) possession factors, such as a token or text message on a mobile phone; or

c) inherence factors, such as a biometric characteristic.

6° **nonpublic information**: all electronic information that is not Publicly Available Information and is:

a) business related information of the bank, the tampering with which, o unauthorized disclosure access or use of which would cause a materia adverse impact to the business, operations o security of the bank;

b) any information concerning an individual which because of name, number personal mark, or othe identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) socia security number, (ii drivers' license number o non-driver identification card number, (iii) accoun number, credit or debit card number, (iv) any security

code, access code o
password that would permi
access to an individual'
financial account, or (v
biometric records;

c) any information or data except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

7° **penetration Testing**: a tes methodology in which assessors attemp to circumvent or defeat the security features of an information system by attempting penetration of databases o

controls from outside or inside the bank's information systems.

8° **publicly Available Information**: any information that a bank has a reasonable basis to believe is lawfully made available to the general public from: the Government or local government records; widely distributed media; or disclosures to the general public that are required to be made by the law.

9° **risk-based authentication**: any risk based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

10° **third party service provider(s)**: a Person that (i) is not an Affiliate of the bank, (ii) provides services to the bank and (iii) maintains, processes or otherwise is permitted access to

Nonpublic Information through its provision of services to the bank.

Article 3: Banking primary data location

Any bank lincensed by the Central Bank must maintain its primary data on the territory of the Republic of Rwanda.

CHAPTER II: REGULATORY REQUIREMENTS

Article 4: Board and Senior Management Cybersecurity Responsibilities

(4.1) Information Security Governance must be the responsibility of the Board of Directors and Senior Management. Each bank must have a comprehensive information security governance framework consisting of the following:

a) cybersecurity strategy linked with business objectives;

b) governing security program that address each aspect of the strategy, controls and regulations;

c)a complete set of standards for each policy to ensure procedures and guidelines comply with the policy;

d) an effective organization structure void of conflict of interest with sufficient authority and adequate resources;

e)metrics and monitoring processes to ensure compliance, feedback on effectiveness and provide the basis for appropriate management decisions;

(4.2) **Expertise at the Board Level**: Each bank must have IT Committee at the Board level to give advice on strategic direction on IT and to review IT investments on Board's behalf.

(4.3) **Powers of IT Committee**: the committee must have the following powers:

a) perform oversight functions

over the IT steering committee at managerial level ;

b) investigate activities within this scope ;

c) seek information from any employee ;

d) obtain outside legal o professional advice ;

e) secure attendance of outsiders with relevant expertise, if i considers necessary ;

f) work in partnership with other board committees and senior management to provide input, review and amend the aligned corporate and IT strategies.

(4.4) Information security strategy implementation, testing and reviews should be planned as part of the Information security program development. The executive committee and the Board must review the security

strategy with the IT Security Unit understand the implications and effects provide feedback on each initiative to achieve strategic objective and allow time for the IT Security Unit representative to respond to the comments and send the next version to the strategic committee for discussion refinement and approval.

The head of the information security or the Chief Executive Officer (CEO) must review approve and communicate the final security strategy document to the intended audience.

(4.5) **IT Steering Committee:** The bank must have an IT Steering Committee with representatives from the IT, HR legal and business lines. Its role must be to assist the Executive Management in implementing IT Security Strategy that has been approved by the Board. It includes prioritization of IT-enabled security investment, reviewing the status of projects (including, resource conflict), monitoring service levels and

improvements, IT service delivery and projects.

(4.6) **IT Security Unit (ISU) :** The bank must establish an IT Security Unit and designate a qualified individual responsible for designing cybersecurity strategy and program, implementing and overseeing the bank's cybersecurity program execution, recommending actions for addressing any noted program shortfalls and enforcing its cybersecurity policy. The unit must also perform regular information security internal assessments and audit.

The responsabilities of the Unit may be undertaken by the bank, one of its affiliates or a third party service provider. To the extent this requirement is met using a third party service provider or an affiliate, the bank must:

a) retain responsibility fo compliance with thi regulation;

b) designate a senior membe of the bank's personne responsible for directio and oversight of the thir party service provider; and

c) require the third part service provider to maintai a cybersecurity progra that protects the bank i accordance with th requirements of thi regulation.

(4.7) **Reporting:** The head of the ISU mus report the Chief Executive Office (CEO) or the senior manager in charg of the cyber security. The Unit mus report on the bank's cybersecurit strategy and program executio identifying emerging materia cybersecurity risks and must consider a least the following:

a) the confidentiality of nonpubli information and the integrity an security of the bank's informatio systems;

b) the bank's/ cybersecurity policie and procedures;

c) emerging material cybersecurity risks to the bank;

d) overall effectiveness of the bank' cybersecurity program achievin security strategy; and

e) material cybersecurity event involving the bank during the tim period addressed by the report ;

Article 5: Cybersecurity strategy an program

(5.1) The bank must maintain a cybersecurity strategy and program designed t protect the confidentiality, integrity an availability of the bank's informatio systems.

(5.2) The cybersecurity strategy must provide the basis for an action plan comprised of cybersecurity program that as implemented, achieve the planned security objectives. The strategy and action plans must contain provision for monitoring as well as defined metrics to determine the level of success.

(5.3) The cybersecurity strategy and program must be based on the Bank's risk assessment and designed to perform at least the following core cybersecurity functions:

a) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the bank's information systems;

b) use defensive infrastructure and the implementation of policies and procedures to protect the bank's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;

c) detect cybersecurity incidents and regularly monitoring of abnormal and unauthorized access or use;

d) respond to identified or detected cybersecurity incidents to mitigate any negative effects;

e) recover from cybersecurity events and restore normal operations and services; and

f) fulfill applicable regulatory reporting obligations.

(5.4) The bank must meet the requirement(s of this regulation by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this regulation, as applicable to the bank.

(5.5) All documentation and information relevant to the bank's cybersecurity strategy and program must be made available to the Central Bank upon request.

Article 6: Cybersecurity Policy

(6.1) The bank must implement and maintain a written policy approved by the bank board of directors, setting forth the bank's policy for the protection of its information systems and nonpublic information stored on those information systems. The cybersecurity policy must be based on the Bank's risk assessment and address at least the following areas of the bank's operations:

a) Information security ;
b) Data governance and classification ;
c) Asset inventory and device management ;

d) Access controls and identity management ;

e) Business continuity and disaster recovery planning and resources ;

f) Systems operations and availability concerns ;

g) Systems, applications and network security;

h) Systems, applications and network monitoring;

i) Application development, acquisition and quality assurance;

j) Physical security and environmental controls;

k) Customer data privacy ;

l) vendor and third party service provider management;

m) Risk management ; and

n) Incident management ;

o) Awerness of staff with regard to sybersecurity ;

p) Integrity requirements requirments of staff dealing with data, systems and networks ;

q) Controls to systems, physical locations containing customer information and tools to monitor access by authorized persons.

Article 7: Penetration Testing and Vulnerability Assessments

The cybersecurity program for each bank must include monitoring and testing, developed in accordance with the bank's risk assessment designed to assess the effectiveness of the bank's cybersecurity program. The monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities bank's must conduct:

a) **Annual penetration testing** of the bank's information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

b) **Bi-annual vulnerability assessments**, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the bank's information systems based on the risk assessment.

Article 8: Audit Trail

Each bank must securely maintain systems that to the extent applicable and based on its risk assessment:

a) are designed to reconstruct materia financial transactions sufficient t support normal operations an obligations of the bank; and

b) include audit trails designed to detec and respond to cybersecurity incident that have reasonable likelihood o materially harming any material part o the normal operations of the bank.

Article 9: Alternative Delivery Channel (ADC) Security Management

(9.1) The bank must ensure adequate Know Your Customer (KYC) procedure during customer registration for onlin and Mobile Financial Services, adequat sensitive data protection, adequat mobile security protection and use training.

(9.2) the core banking systems must b intergeted with National Identificatio system for the customer identit verification mechanism.

(9.3) The bank shall employ security mechanisms that prevent unauthorized access to sensitive data at rest or in transit as contained in this regulation.

Article 10 : Risk Management

10.1) Each bank shall conduct a periodic risk assessment of the bank's information systems sufficient to inform the design of the cybersecurity program as required by this regulation. Such risk assessment shall be updated as reasonably necessary to address changes to the bank's information systems, non public information or business operations.

10.2) The bank's risk assessment must allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the bank's business operations related to cybersecurity, non public information collected or stored information systems utilized and the

availability and effectiveness of controls to protect nonpublic information and information systems.

10.3) The risk assessment must be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

a) Criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the bank;

b) Criteria for the assessment of the confidentiality, integrity, security and availability of the bank's/FI information systems and nonpublic information including the adequacy of existing controls in the context of identified risks; and

c) Acceptance criteria describing how identified risks will be treated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Article 11: Third Party Service Provider

(11.1) The bank must implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers. Such policies and procedures shall be based on the risk assessment of the bank and shall address to the extent applicable:

a) the identification and risk assessment of third party service providers;

b) minimum cybersecurity practices required to be met by such third

party service providers in order fo them to do business with the bank;

c) due diligence processes used t evaluate the adequacy o cybersecurity practices of such third party service providers; and

d) periodic assessment of such third party service providers based on th risk they present and the continued adequacy of their cybersecurity practices.

(11.2) Such policies and procedures mus include relevant guidelines for du diligence and/or contractual protection relating to third party service provider including to the extent applicabl guidelines addressing:

a) the third party service provider' policies and procedures for acces controls, including its use of multi factor authentication as required b

Article 12 of this Regulation, to limit access to relevant Information systems and non-public information;

b) the third party service provider's policies and procedures for use of encryption as required by Article 12 of this Regulation to protect non-public information in transit and at rest;

c) notice to be provided to the bank in the event of a cybersecurity incident directly impacting the bank's/FI information systems or the bank's non-public information being held by the third party service provider and

d) representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the bank's/FI information systems or non-public information.

Article 12: Multi-Factor Authentication

(12.1) Based on its risk assessment, each bank shall use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems.

(12.2) Multi-factor authentication shall be utilized for any individual accessing the bank's internal networks from an external network, unless the bank's head of ISU has approved in writing the use of reasonably equivalent or more secure access controls.

Article 13: Limitations on Data Retention

As part of its cybersecurity program, each bank must have a data retention policy for the secure keeping and disposal on a periodic basis of any nonpublic information identified as per their Risk assessment, except where such information is otherwise required to be retained by law or regulation.

Article 14: User Training and Monitoring

(14.1) As part of its cybersecurity program each bank must:

a) design a consistent and updated security awareness program in line with institution's risk assessment, strategy and current cybersecurity threats and trends ;

b) provide regular cybersecurity awareness training for all personnel that interacts with institution's information system including but not limited to staff, interns, third party ;

c) evaluate the effectiveness of the awareness training through regular quizes and test simulations.

Article 15: Encryption of Non-public Information

(15.1) As part of its cybersecurity program based on its risk assessment, each bank shall implement controls, including encryption, to protect nonpublic information held or transmitted by the bank both in transit over external networks and at rest.

(15.2) To the extent a bank determines that encryption of nonpublic information in transit over external networks is infeasible, the bank may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the bank's head of ISU.

(15.3) To the extent a bank determines that encryption of Nonpublic Information at rest is infeasible, the bank may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the bank's head of ISU.

(15.4) To the extent that a bank is utilizing compensating controls as mentioned above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by ISU at least annually.

Article 16 Incident Response and business continuity management

(16.1) As part of its cybersecurity program each bank shall establish a written incident response and business continuity management plan designed to promptly respond to, and recover from any cybersecurity incident materially affecting the confidentiality, integrity or availability of the bank's information systems or the continuing functionality of any aspect of the bank's business or operations.

(16.2) Such incident response and business continuity management plan shall address the following areas:

a) the internal processes for responding to cybersecurity incident and disasters;

b) the goals of the incident response and business continuity plans;

c) the definition of clear roles responsibilities and levels of decision-making authority;

d) external and internal communications and information sharing;

e) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

f) documentation and reporting regarding cybersecurity events and related incident response activities and

g) the evaluation and revision as necessary of the incident response

and business continuity plans following a cybersecurity event.

Article 17 Notices to the Central Bank

(17.1) The bank must notify Central Bank as promptly as possible within a period not exceeding two (2) hours from the occurrence of the incident or from a determination that a cybersecurity incident has occurred that is either of the following:

a) cybersecurity incident that may prevent a specific bank branch from continuing its normal operations for customer-facing transactions, and

b) cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the bank.

(17.2) The Bank must submit to the Centra Bank the full incident report within 2 hours from the occurrence of th incident.

(17.3) The bank shall submit to the Centra Bank on annual basis a writte statement as per the appendix certifyin that the bank cyber securtiy program i in compliance with the requirements se forth in this Regulation. The statemen shall be submitted not later than 15t January of each year.

Article 18 Confidentiality

Information provided by a bank pursuant to thi Regulation is subject to exemptions fro disclosure under the Banking Law or any othe applicable law.

CHAPTER III: MISCELLANEOUS AN FINAL PROVISIONS

Article 19 Penalties and administrativ sanctions

Where the bank fails to satisfy any of th requirements of this Regulation, the Centra Bank may apply any sanctions available unde relevant provisions of the Law concernin

organization of banking and/or provisions of a relevant regulation.

Article 20 : Deadline for conforming to certain provisions of this regulation

Banks shall have eighteen (18) months as from the entry into force of this regulation to conform their functioning with the provisions of article 3 of this regulation.

Banks are given a maximun of six (6) months to comply with provisions of Article 4, 5 and 6 of this regulation, starting from the date of its publication in the Official Gazette of the Republic of Rwanda.

Article 21: Repealing provisions

All previous provisions contrary to this Regulation are hereby repealed.

Article 22: Drafting, consideration and approval of this Regulation

This Regulation was drafted, considered and approved in English.

Article 23: Commencement

This regulation shall come into force on the date of its publication in the Official Gazette of the Republic of Rwanda.

Done at Kigali, on 24/01/2018

(sé)
RWANGOMBWA John
Governor

Rwanda Cybersecurity Regulation

ank] certifies:

ficer(s)) has reviewed documents, reports, certif

or entities as necessary;

ame of Senior Officer(s)] knowledge, the Cyb

or Senior Officer(s)) Compliance Finding for the

ies with this Regulation _____(regulation nymb

or the CEO)

e: _____