REGULATIONS N^{o} 001/R/TD-ICS/RURA/016 OF 06/05/2016 GOVERNING TELECOM NETWORK SECURITY IN RWANDA

ADOPTED BY THE

REGULATORY BOARD

OF

RWANDA UTILITIES REGULATORY AUTHORITY (RURA)

TABLE OF CONTENTS

REGULATIONS GOVERNING TELECOM NETWORK SECURITY IN RWANDA

Preamble

The Rwanda Utilities Regulatory Board

Pursuant to the law n° 44/2001 of 30/11/2001 governing telecommunications especially in Articles 54 ; 55 and 56;

Pursuant to the law n° 04/2013 of 08/02/2013 relating to access to information in Rwanda especially in Article 4;

Pursuant to the law n° 09/2013 of 01/03/2013 establishing Rwanda Utilities Regulatory Authority (RURA) and determining its mission, powers, organization and functioning**,** especially in Article 2;

Pursuant to the law n° 60/2013 of 22/08/2013 regulating the Interception of Communications especially in Article 5;

Pursuant to the Prime Minister's Order n°90/03 of 11/09/2014 determining modalities for the enforcement of the law regulating interception of communication especially in Articles 8 and 9;

Conscious that any attack on the telecommunication network could lead to lose the essential communication services and thus all licensed telecom operators must fight security threats to secure the subscribers communication both at national and international level;

Due to the dynamic nature of the telecom network and new changing threats to security and resilience of the networks, today's cyber adversaries and malicious individuals are constantly sharpening and evolving their capabilities to exploit the new vulnerabilities of the network ;

Emphasizing the necessity to strengthen the subscriber's privacy maintained at all levels;

Considering that it is important to build an environment that is well secured by putting in place a legal and regulatory information security framework;

The Regulatory Board, upon due consideration and deliberation in its meeting of **06/05/2016**;

HEREBY issues the following Regulations;

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Regulation

The purpose of this Regulation is to secure the Telecommunication networks and its subscribers and the critical communication infrastructure to ensure confidentiality, Integrity and the availability elements of Rwanda.

Article 2: Definitions of terms

For the purpose of this Regulation, terms below shall have the following meanings:

1. **Caller ID:** Is a telephone service, available in analog and digital phone systems, that transmits a caller's number to the called party's telephone equipment during the ringing signal, or when the call is being set up but before the call is answered. Where available, caller ID can also provide a name associated with the calling telephone number;
2. **CSIRT:** Computer Security Incident Response Team set up by Government of Rwanda to take care of any computer related incidents;
3. **Customer personal information:** The Information generated through regular calls, SMS and browsing history such as Call Data Record or Billing record and SMS details;
4. **Data** : Electronic representations of information in any form;
5. **Data traffic:** data in a network. In mobile networks, data is encapsulated in network packets;
6. **DoS:** A denial-of-Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users;
7. **DDoS:** A distribution Denial of Service (DDoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet;
8. **Handset:** A Handset or mobile phone also known as a cellular phone, cell phone, hand phone, or simply a phone is a phone that can make and receive telephone calls over a radio link while moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network;

9. **Infrastructure and services**: Includes data, system, equipment, networks and applications;
10. **Information Security:** It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction;
11. **ISO**: International Standard Organisation;
12. **IEC**: International Electro Technical Commission;
13. **KPI:** A ke**y** Performance Indicator (KPI) is a business metric used to evaluate factors that are crucial to the success of an organization or service provided;
14. **Licensed Telecom Operator:** A Telecommunication Service provider holding a valid License issued by the Regulatory Authority;
15. **Licensed Internet Service Provider:** a company licensed that provides retail access to the Internet for members of the public, or for businesses and other organizations.
16. **Licensee :** A Telecommunication Service provider or Internet Service Provider holding a valid License issued by the Regulatory Authority;
17. **Network facilities:** Any elements used in connection with the provision of public electronic communication networks;
18. **NMS:** A network Management System (NMS) is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework;
19. **Regulatory Authority:** Rwanda Utilities Regulatory Authority as established by the Law nº 09/2013 of 01/03/2013;
20. **SMS:** Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages
21. **SLA:** A service-Level Agreement (SLA) is a part of a service contract, where a service is formally defined. Particular aspects of the service - scope, quality, responsibilities - are agreed between the service provider and the service user;
22. **Subscriber:** A person who is a party to a contract with a provider of public electronic communication services for the supply of such services. However a subscriber shall be a user owning a terminal equipment for the purpose of receiving services from electronic

communication network but not providing public communications networks or publicly available electronic communications services;

23. **Telecommunication Service Provider :**A person providing public electronic communications services;
24. **Unauthorised person:** is any person who is not authorised to access subscriber's information as required by the Law(s) into force.
25. **VAS:** A Value-Added Service (VAS) is a popular telecommunications industry term for non-core services, or in short, all services beyond standard voice calls, SMS, DATA services and fax transmissions.

Article 3: Scope of this Regulation

This Regulation shall apply to all infrastructure and services provided by the Licensees.

Article 4: Exclusion

Licensed Internet Service Providers are exempted from the articles which are specific to mobile phone services, where they are not offering mobile phone based services otherwise all the controls are applicable.

Article 5: Objectives of this Regulation

The objectives of this Regulation are the following:

(a) To ensure that Licensed Internet Service Providers and Telecommunication Network Service Providers and its subscribers are under a regulated and secure environment;
(b) To ensure that the Licensed Internet Service Providers and telecommunication Service Provider delivers the secured services;
(c) To deal with the monitoring and control of the security state of the system; and
(d) To assist the Licensed Internet Service Providers and telecommunication Service Providers to protect their infrastructure and the Subscriber's interests and
(e) To ensure that the Licensed Internet Service Providers and telecommunication Service Providers services are prevented from being interrupted, corrupted or denied.

CHAPTER II: RESPONSIBILITIES OF LICENSEES AND SUBSCRIBERS

Article 6: Responsibilities of Licensees

Under this regulation, the licensees shall have the following responsibilities:

(a) Ensuring security of the information captured, stored, processed and transmitted in their networks ;
(b) Implementing, operating, maintaining and monitoring the controls mentioned in these Regulations and required International standards such as **ISO/IEC 27001 or ISO/IEC 27011;**
(c) Developing, Documenting and following well defined secured process;
(d) Protecting Subscriber's interests and gaining their confidence by providing secured communication services and value added services; and
(e) Complying with any legal and regulatory requirements provided under these Regulations.

Article 7: Responsibilities of Subscribers

The subscribers have the following Responsibilities:

(a) Take care of their actions while they are using mobile for communication;
(b) To protect their security and always check the SIM cards registered under their names;
(c) Make the backup and recovery of the data on her/his handset ; and
(d) Have an Antivirus on his/her handset if deemed necessary; and
(e) Securing the information stored in their handset or any devices using password or any other authentication method.

CHAPTER III: SECURITY CONTROLS TO PROTECT THE NETWORK FACILITIES OF THE LICENSEES AND SUBSCRIBER'S INFORMATIONS

Article 8: Security Measures

The Licensees shall take all the required security measures to guarantee the confidentiality, integrity, availability of their networks and services for the entire duration of their Licenses.

Appropriate technical and organisational measures must be taken by the Licensees to ensure a level of security appropriate to the risks posed. Those security measures must be appropriate for

preventing or minimising the impact of security incidents of the subsribers and interconnected networks.

Article 9: Appropriate security controls

The Licensees shall ensure that appropriate security controls are set in their network against various known and unknown threats. A comprehensive Information Security framework shall include the essential components such as;

(a) Risk Assessment;
(b) Configuration Management;
(c) Change Management;
(d) Incident Management;
(e) Secured application acquisition, development and maintenance;
(f) Business continuity plan and Disaster recovery plan;
(g) Vulnerability assessment and Audit;
(h) Internal and external penetration testing and
(i) Legal and Regulatory compliance identifying, maintaining and monitoring.

Article 10: Establishment of Layers in the Network facilities

Any network facility of the licensees must have at least three (3) layers which are as follows:

1) Management plane;
2) Signalling plane; and
3) Data plane.

Article 11: Importance of Layers in the Network facilities

The management plane has the role of securing the network traffic management and network operation while the signalling plane used for signalling and routing the traffic.
The data plane has the role of delivering data services to the customer devices.

Article 12: Protection of the management Plane

To protect the management plane, any licensee must take into consideration the following:

(a) To have and follow well defined information Security policy and Procedures;
(b) To ensure segregation of duties in every process;
(c) To ensure the segregation of Networks;

(d) To prevent unauthorised and uncontrolled access to nodes and related application;
(e) To secure the customer information such as personal information such as call data record, billing and other relevant information;
(f) To ensure a regular backup; To define access control management for employees, subscribers and vendors based on the least privilege guidance and ensure the non-repudiation by implementing strong authentication controls;
(g) To conduct a regular log review of devices access and application access;
(h) To ensure the application security by secure development and performing security testing ;
(i) To have and follow well defined SIM card registration process to identify the subscriber identity;
(j) To ensure security hardening of all nodes, devices, systems and applications ;
(k) To allow tested and secured Value added services;
(l) To conduct regular audit on all Value added services;
(m) To regularly provide awareness to its employees ;
(n) To provide adequate contingency plan and arrangements in their networks ; and
(o) To provide any protection required by international standards and best practices. Remote access to nodes and systems for configuring, patching, backup, logging, provisioning, billing and subscriber care shall be documented, controlled and monitored.

Under this provision, Regular backup requires that Configuration be backed up whenever any change is incorporated in it so as to maintain the backed up configuration as exactly the same as the running configuration immediately prior to the change. Other information such as customer related Logs, business and network information backup shall have daily, Monthly and yearly backups.

Article 13: Protection of the Signalling Plane

The signalling plane is used for call setup and subscriber service delivery. To this effect the licensee must always protect their subscribers against:

(a) Passive and active interception;
(b) Impersonation ; and
(c) Subscriber tracking.

To enhance the security of the subscribers, the licensee must:

i) Verify and validate all signalling partners;
ii) Validate all external input comes from signalling partners;
iii) Prevent signalling points from being addressable from the either the data plane or being accessible from outside of the Control plane;
iv) Implement controls to validate the end devices on operator's networks to ensure that no unauthorized devices are able to connect;

v) Ensure that all the incoming and outgoing traffic are validated and filtered;
vi) Have SMS firewall to control and monitoring SMS traffic; and
vii) Security hardening the devices and applications.

Article 14: Protection of the data plane

The data plane must be protected by the licensed telecom service providers to avoid cyber attack and data breach and mitigate the risk on their network.

Article 15: Required Minimum controls for data plane

The Licensees are required to put in place the following minimum controls which include but not limited to:

i) Filtering and monitoring network traffic;
ii) Protection against DoS and DDoS attacks;
iii) Segregation of network and ensure data plane traffic that not affecting other planes ;
iv) Monitoring and verifying all traffic including their originating source;
v) Implement controls to identify subscriber traffic and activities;
vi) Use traffic restriction where deemed necessary; and
vii) Capacity of being able to prevent and monitor any network anomaly.

Article 16: Protection of Subscribers Privacy

Any licensee shall ensure that:

(a) Subscribers' information such as voice, SMS, data including Call data record, Billing information must be processed, stored and transmitted securely to ensure Subscribers privacy;
(b) Subscribers' information are not available to any unauthorised person;
(c) The control is in place to monitor and restrict subscribers' information from any unauthorised access; and all calls should have caller identification.
(d) Any access to customer information should be logged such that can be traced if required;
(e) Subscriber's information are not transferred, stored or processed outside of the Republic of Rwanda.

Article 17: Call ID information

Caller ID masking feature shall be allowed by the Licensee only after getting approval from the Regulatory Authority. A List of subscribers having such facility must be updated from time to time and made available to the Regulatory Authority.

Article 18: Outsourcing the System and Operation to a third party

All Licensees willing or having outsourced their systems and operation to any third party must extend their security framework to the third party.

The Licensee shall seek approval from the Regulatory Authority before outsourcing any of its services or operation to any third party.

The Licensee is required to have a Rwandan native as its Chief Technical Officer (CTO) Chief Information officer (CIO) or equivalent functions, responsible for its network technical and Information technology infrastructure, systems planning and operations.

Article 19: Conditions of outsourcing the System and Operation to a third party

After the approval of outsourcing the system and operation to any third party, the licensee is required to:

(a) Define detailed security process for selection of third party;
(b) Design contracts with third parties containing information security requirements and KPIs or SLAs ;
(c) Implement a structured risk assessment process with third parties;
(d) Background verification of all the third parties Organisation and employees ;
(e) Aligning the security policy of the third parties with the Licensed operators security requirements ;
(f) Conducting regular review and audit on the third parties ; and
(g) Extending the business continuity beyond organizational boundaries to third parties.

CHAPTER IV: SECURITY ASSESSEMENT AND AUDIT OF NETWORK OF LICENSEES

Article 20: Security Assessment of all planes

To prevent any threats before it becomes real, all licensed telecom operators shall perform once in a year vulnerability assessment and penetration testing for all planes to identify the weakness and fix it in a timely manner.

Article 21: Vulnerability Assessment

To conduct the vulnerability assessment of their network, the licensees must:

(a) Have test devices, nodes and applications with manual or automated tools;
(b) Conducting vulnerability assessment on all the plane twice a year;
(c) Perform security testing prior to systems being granted approval to move into production;
(d) Fix the identified vulnerabilities by applying patch or secure configuration ; and
(e) Ensure that all planes are secure by conducting regular risk assessments on each plane to identify and respond to unacceptable risks.

Article 22: Internal Audit

All Licensees must conduct at least twice a year technical and process audit to verify the effectiveness of the implemented security controls such as management, technical and physical controls.

The Licensee shall measure the effectiveness of implemented controls. Any controls shortfall or failure Operators must remediate as soon as possible and remediation should not extend beyond three (3) months. Any extension to this period is subject to Regulatory Authority's approval.

Article 23: Compensatory Controls

Where there is management decision required or delay in acquisition to correct controls deficiencies, the licensed telecom operator shall identify appropriate compensatory controls and implement the same.

Article 24: Submission of the Assessment and audit Report

All licensees must submit the Audit and assessment reports to the Regulatory Authority not later than thirty (30) calendar days after the assessment conducted by licensees.

Article 25: Remediation Plan

The remediation plan of each licensed telecom operators must be submitted to the Regulatory Authority along with audit reports.

Article 26: **Regulatory Authority Audit**

All Licensees shall comply to this regulation and the Regulatory Authority shall conduct audit yearly once. The audit findings shall be remediate and provide the status of the findings.

All licensees are required to facilitate the auditors by providing requested information and evidence.

In the event of conducting regular audit, the Regulatory Authority shall notify the Licensees two (2) weeks prior to such audit.

CHAPTER V: EFFECTIVE MANAGEMENT OF INCIDENTS

Article 27: Incident Management

The Licensee must protect their infrastructure which include but not limited to:

(a) Implementation of a security incident reporting and handling process, Incident Management process and training of its employees on how to use the processes in the event of any adverse event.
(b) Guidelines for identifying any incident as a security incident;
(c) Communication channels to be used for reporting the security incident;
(d) Recording security incidents reported;
(e) Assigning severity to security incidents;
(f) Escalation mechanism for security incidents;
(g) Resolution and closure of incidents;
(h) Root cause analysis;
(i) Monthly report to business for root cause analysis; and
(j) Create an internal incident management team to work in cooperation with government CSIRT to deal with security incidents effectively.

The categorisation of incidents under this provision is explained in annex of this Regulation.

Article 28: Sharing Security incident

Every Licensee must immediately share with the Regulatory Authority any security incidents which have occurred and considered as critical and major as defined in annex of this Regulation.

For moderate incidents, a monthly report shall be submitted by the Licensee by using electronic communication channels approved by the Regulatory Authority.

The Regulatory Authority shall assess such incident(s) and ensure that this information is utilized by the licensee and other competent organs to avoid similar incidents in future.

Article 29: Monitoring and Compliance

All Licensees shall monitor and comply with all security standards provided under these regulations to maintain a secured system infrastructure.

The Regulatory Authority shall conduct audit in all licensees, at least once a year, for compliance of this Regulation.

CHAPTER VI: ADMINISTRATIVE SANCTIONS

Article 30: Non-compliance with the Enforcement notice

Every Licensee who does not comply with the enforcement notice issued by the Regulatory Authority in accordance with the provisions of this Regulation shall be liable to an administrative fine of between one million (1,000,000) and five million (5,000,000) Rwanda francs. Failing to do so, he/she shall be liable to an administrative fine of five hundred thousand (500,000) Rwanda francs per day as from the date he/she received an enforcement notice for complying with the requirements.

Article 31: Refusal to provide information related to security incident

If a Licensee fails or refuses to provide timely the information related to security incident or gives partial or false information related to the security incidents to the Regulatory Authority or fails to provide information related to security incident in accordance with the relevant procedure or within the planned timeframe, he/she shall be liable to an administrative fine of between five hundred thousand (500,000) and one million (1,000,000) Rwanda francs.

Article 32: Delay to submit the reports

Every licensee that delays to submit intentionally the audit plan report, the audit report and remediation plan to the Regulatory Authority as provided under this Regulation shall be liable to an administrative fine of between two hundred thousand (200,000) and one million (1,000,000) Rwanda francs.

Article 33: Non –compliance to any Requirement of this Regulation

Every Licensee who does not comply with any other requirement of this Regulation shall be liable to an administrative fine of between one million (1,000,000) and five million (5,000,000) Rwanda francs.

CHAPTER VII: FINAL PROVISIONS

Article 34: Transition period

All existing Licensees are required to comply with this regulation in a period of six (6) months effective from the date of signature by the Chairperson of the Regulatory Board.

Article 35: Repealing provision

All prior regulatory provisions contrary to this regulation are hereby repealed.

Article 36: Commencement

This regulation shall come into force on the date of its signature by the Chairperson of the Regulatory Board.

Done at Kigali on, 02/06/2016

(Sé)

Eng. Coletha U. RUHAMYA
Chairperson of the Regulatory Board

Annex: Management of Incidents

Incident Metrics			
	Core Network Services (Critical)	VAS (Major)	Non Urgent Services (Minor)
Entire Network (Critical)	Critical	Major	Minor
Partial Network (Major)	Critical	Major	Minor
Individual(Minor)	Moderate	Minor	Minor

(Sé)

Eng. Coletha U. RUHAMYA
Chairperson of the Regulatory Board