RWANDA UTILITIES REGULATORY AUTHORITY
P.O BOX 7289 KIGALI,
Tel: +250 584562, Fax: +250 584563
E-mail: info@rura.rw
Website: www.rura.rw

CYBERSECURITY REGULATION N° 010/R/CR-CSI/RURA/020 OF 29/05/2020

TABLE OF CONTENTS

Preamble

The Rwanda Utilities Regulatory Board

Pursuant to law n° 24/2016 of 18/06/2016 governing information and communication technologies especially in Articles 123,124,125,126 and 127;

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

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

Pursuant to Law Nº 60/2018 of 22/8/2018 on prevention and punishment of cyber crimes;

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;

Considering deliberations from the consultative meeting held on October 2nd, 2019 with stakeholders;

The Regulatory Board, upon due consideration and deliberation in its meeting of **May 29th, 2020**;

HEREBY issues the following Regulation;

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Regulation

The purpose of this Regulation is to secure networks, their subscribers and the critical communication infrastructure to ensure the confidentiality, integrity and availability of networks and systems in Rwanda.

Article 2: Definitions of Terms

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

1. **Application Service Provider**: any licensed operator offering all forms of ICT application to end users by using the infrastructure of other licensed Network Service Providers;
2. **Caller Identification:** a telephone service, available in analogue and digital phone systems, that transmits a caller's number and the name associated with the calling telephone number where possible 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;
3. **Compliance Audit**: Is a comprehensive review of an organization's adherence to this regulation;
4. **Critical Incident:** An event that results in a partial loss of core service and entirely affects value added-services;
5. **Data:** Electronic representations of information in any form;
6. **Digital Footprint:** refers to one's unique set of traceable digital activities, actions, contributions and communications that are manifested on the Internet or on digital devices;
7. **Independent Security Audit**: a comprehensive assessment conducted by external party, which is allowed, in order to assess the current condition of Information Security in the business of the licensee and to plan timely actions in order to increase the level of security.
8. **Information Security:** The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction;
9. **Infrastructure and services**: Include data, system, equipment, networks and applications;
10. **ISO/IEC**: Is a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its purpose is to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT);

11. **IT:** Information Technology;
12. **KPI:** Key Performance Indicator is a business metric used to evaluate factors that are crucial to the success of an organization or service provided;
13. **Licensed Internet Service Provider:** A licensed company that provides retail access to the Internet for members of the public, or for businesses and other organizations;
14. **Licensed Telecom Operator:** A Telecommunication Service provider holding a valid License issued by the Regulatory Authority;
15. **Licensee:** a person who holds a license issued by the Regulatory Authority under this regulation;
16. **Major Incident:** An event that causes a partial loss of value-added services;
17. **Minor Incident:** An event that has impact on some subscriber, and limits their access to value-added services;
18. **Moderate Incident:** An event that has a partial impact on core services of the subscriber.
19. **Network Facilities:** Any elements used in connection with the provision of public electronic communication networks;
20. **Network Infrastructure Service Providers**: Licensees who own, operate or provide any form of active or passive physical infrastructure used for carrying or providing services, applications and content;
21. **Network Service Providers:** Licensees who provide services to those using electronic communications networks**.** These include Internet Service Providers who do not own infrastructure;
22. **Network Management System (NMS):** 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;
23. **Personal data:** Any information relating to an identified or identifiable individual by reference to any number of his/her identifications or to his or her physical, physiological, mental, economic, cultural or social identity;
24. **Public Key Infrastructure (PKI):** A system of Certification Service Provider that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography;
25. **Regulatory Authority:** Rwanda Utilities Regulatory Authority as established by the Law nº 09/2013 of 01/03/2013;

26. **Security 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.
27. **Service-Level Agreement (SLA):** 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;
28. **Short Message Service (SMS):** A text messaging service component of phone, Web, or mobile communication systems, which uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages;
29. **Signalling/Control plane:** A layer where specific communication protocols are used to establish calls and sessions between systems, subscribers and service providers;
30. **Standards:** for the purpose of this regulation, standards refer to required international standards such as ISMS ISO/IEC 27001: 2013 or ISO/IEC 27011 as it may be amended from time to time;
31. **Subscriber Personal Information:** Any information generated through regular calls, SMS and transactions history such as Call data record, mobile financial services or Billing record and SMS details;
32. **Subscriber:** Any person who is a party to a contract with a provider of public electronic communications services for the supply of such services;
33. **System:** A set up of ICT components comprising of hardware, software and networking elements that are owned, controlled, operated, leased or otherwise relied on by the service provider;
34. **Telecommunication Service Provider:** An entity providing public electronic communications services;
35. **Third Party:** An individual or company supplying products or services to the service provider (licensee) or on the behalf of the licensee;
36. **Traffic Data:** any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication; In mobile networks, data is encapsulated in network packets;
37. **Unauthorized person:** is any person who is not authorized to access subscriber's information as required by the laws and regulations in force;
38. **Urgent incidents:** Incidents shall be considered as "urgent" if they meet any of the following criteria:

(a) all incidents affecting services to 25% of the licensee's total number of subscribers on the affected service.

(b) an incident that results in loss of core services and affects the entire Value-Added Services;

(c) incidents attracting national mainstream media coverage;

(d) incidents affecting government or public sector services;

39. User: any person using or requesting publicly available electronic communications services.

Article 3: Scope of this Regulation

This Regulation shall apply to all ICT infrastructure and services provided to the public by the licensee.

Article 4: Objectives of this Regulation

The objective of this Regulation is:

(a) to ensure that all licensees and their subscribers are under a controlled and secure environment;

(b) to ensure that the licensees deliver secured services;

(c) to deal with the monitoring and control of the security state of systems;

(d) to ensure that the licensees protect their systems and subscribers' interests; and

(e) to ensure that the licensees' services are prevented from being interrupted, corrupted or denied.

CHAPTER II: RESPONSIBILITIES OF LICENSEES AND SUBSCRIBERS

Article 5: Responsibilities of Licensees

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

(a) ensuring security of the information captured, stored, processed and transmitted in or through their networks and systems;

(b) implementing, operating, maintaining and monitoring the controls mentioned in this regulation and required international standards such as ISO/IEC 27001: 2013 or ISO/IEC 27011 as it may be amended from time to time;

(c) developing, documenting and following well defined secured processes;
(d) protecting subscribers' interests and gaining their confidence by providing secured systems and services;
(e) implementing and maintaining appropriate technical and organizational measures to secure systems and services provided to subscribers;
(f) ensure that users are adequately protected while using provided services.
(g) reporting of security incidents to the Regulatory Authority;
(h) complying with all legal and regulatory requirements provided under this regulation and other laws in Rwanda.
(i) issue cyber security related advisories to subscribers when risks have been identified in the specific licensee services.

Article 6: Responsibilities of Subscribers

The subscribers using ICT services shall take actions comprising of but not limited to the following:

(a) always verify and ensure that their digital credentials such as sim registration details, Personal Identification Number (PIN), passwords, user accounts, are safely protected;
(b) apply necessary software patches and backup the data on their devices; and
(c) have antimalware on their devices where possible.

CHAPTER III: SECURITY CONTROLS TO PROTECT THE NETWORK, SYSTEMS OF LICENSEES AND SUBSCRIBER'S INFORMATION

Article 7: Security Measures

The licensee must take all required security measures to guarantee the confidentiality, integrity and availability of their network, systems and services for the entire duration of the License.

The Licensee is required to implement and maintain appropriate technical and organizational measures to secure systems and services provided to their subscribers. Such measures must be implemented to support subscribers in securing their personal data against unauthorized processing and accidental or unlawful loss, access or disclosure.

These security measures must be adequate to prevent or minimize the impact of security incidents on the subscribers, interconnected networks systems and services.

Article 8: Appropriate Security Controls

The Licensee shall ensure that appropriate security controls are clearly documented and set in their network and systems against various known and unknown threats. A comprehensive Information Security Management System (ISMS) must be implemented including the essential components hereunder:

(a) risk assessment;
(b) information security policies
(c) asset management
(d) access control
(e) communications and operations management
(f) configuration management;
(g) change management;
(h) incident management;
(i) secured application acquisition, development and maintenance;
(j) business continuity plan and disaster recovery plan;
(k) vulnerability assessment and audit;
(l) internal and external penetration testing by auditors approved by the regulatory authority;
(m) legal and regulatory compliance identifying, maintaining and monitoring;
(n) cryptographic algorithm management;
(o) human resources security; and
(p) backup management.

Article 9: Establishment of Layers in Network Facilities

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

(a) management plane;
(b) signalling/ control plane or communication protocol; and
(c) data plane.

Article 10: 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 is used for signalling and routing the traffic. The data plane has the role of delivering data services to the subscriber devices.

Article 11: Protection of the Management Plane

To protect the management plane, all licensees must:

(a) have and follow well defined industry information security policies and procedures;
(b) ensure segregation of duties in every process;
(c) ensure the segregation of networks and systems;
(d) prevent unauthorized and uncontrolled access to network and systems including related applications;
(e) secure the subscriber information such as personal information including but not limited to Call Data Records (CDRs) where applicable, billing and other relevant information;
(f) ensure a regular backup;
(g) define access control management for employees, subscribers and vendors based on the least privilege guidance and ensure non-repudiation by implementing strong authentication controls;
(h) conduct a regular log review of devices access and application access;
(i) ensure the application security through secure development and performing security testing;
(j) have and follow well defined Know Your Customer (KYC) procedures
(k) ensure security hardening of all nodes, devices, systems and applications;
(l) only allow deployment and/or integration of tested and secured systems, applications and services;
(m) ensure that internal security policies are regularly updated and approved by the regulatory Authority
(n) conduct regular audit on all systems, applications and services;
(o) share information to subscribers whenever an incident occurs;
(p) regularly provide awareness on security incidents to its employees depending on their roles and responsibilities and ensure means of evaluation of the performance of employees as a result of such awareness;

(q) inform subscribers of the risks to the security of provided services, appropriate measures that the subscriber may take to safeguard against the risks and the likely costs to the subscriber involved in the taking of such measures. Information provided for this purpose must be provided to the subscriber free of any charge other than the cost that the subscriber would have incurred for accessing the information.
(r) provide adequate contingency plans and arrangements in their systems, applications and services;
(s) maintain, document, control and monitor all access logs of all network, systems and applications;
(t) document, control and monitor all remote access to nodes and systems for configuring, patching, backup, logging, provisioning, billing and subscriber care; and
(u) implement controls to prevent fraudulent access to their network and systems.

Under this provision, the licensee shall ensure regular network and system configuration backups and, whenever any change is incorporated, the backed-up configurations must be identical to the running configurations prior to the change.

Other subscriber related information such as Logs, business and network information backups must have daily, monthly and annual plans.

Article 12: Protection of the Signalling or Control Plane

The licensee must always ensure protection of their subscribers against:

(a) passive and active interception;
(b) impersonation; and
(c) subscriber tracking and traceability of digital footprints.

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

(a) verify and validate all signalling partners;
(b) validate all external input originating from signalling partners;
(c) prevent signalling points from being addressable from the either the data plane or being accessible from outside of the control plane;
(d) implement controls to validate the end devices on operator's networks to ensure that no unauthorized devices are able to connect;
(e) ensure that all the incoming and outgoing traffic are validated and filtered;
(f) have SMS firewall to control and monitoring SMS traffic where applicable and;

(g) ensure security hardening of devices and applications.

Article 13: Protection of the Data Plane

The licensee shall protect the data plane to avoid cyber-attack and data breaches as well as mitigate the risk on their network, systems and services.

Article 14: Required Minimum Controls for Data Plane

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

(a) filter and monitor traffic data;
(b) ensure data confidentiality, integrity and availability;
(c) monitor and verify all traffic including their originating source;
(d) ensure implementation of intrusion, detection, and prevention systems to protect against network intrusions and unauthorised access;
(e) use traffic restriction where deemed necessary;
(f) ensure capacity to identify and monitor any anomalies;
(g) ensure subscriber's information transferred or accessed through any channel or Virtual Private Network (VPN) links shall be protected with industry recommended encryption standards to ensure the authenticity and confidentiality of data; and
(h) use PKI Digital certificates to ensure secure electronic transactions where applicable.

Article 15: Management and Protection of Networks and Systems

All networks, systems and applications of the licensee shall not be managed, hosted, remotely accessed or located outside of the Republic of Rwanda unless explicitly authorized by the Regulatory Authority.

Article 16: Call ID Information

Where applicable, all local incoming calls originating from within Rwanda shall have Caller Identification. Any masking feature shall not be allowed except for those approved by the Regulatory Authority.

Any subscriber who wishes to have the masking feature applied to his/her number must seek authorisation from the Regulatory Authority and if granted, submit the authorisation to the Licensee for implementation.

Article 17: Outsourcing Systems and Operations to a Third Party

Before outsourcing any of its systems, operations or services to any third party, the licensee shall seek approval from the Regulatory Authority and ensure that all third parties are licensed by the Regulatory Authority prior to any contractual engagement.

Any third party who wants to operate on the Rwanda ICT market shall be approved by the Regulatory Authority.

Any Licensee willing or having outsourced their systems and operations to any third party must extend their security framework to the third party.

The Licensee is required to have a Rwandan 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 18: Conditions of Outsourcing Systems and Operations to a Third Party

After the approval to outsource systems and operations 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) perform background verification of all the third parties, organisations and employees' technical skill sets involved in the operations and management of the systems;
(e) align the security policies of the third parties with the Licensee's security requirements;
(f) conduct regular review and audit on the third parties; and
(g) extend the business continuity plans beyond organizational boundaries to third parties.

Article 19: Authorization Procedures

The licensee shall request in writing, authorization or non-objection specified in this regulation to the Regulatory Authority.

The licensee shall justify the reason for the request and provide sufficient information to allow the Regulatory Authority to make appropriate decision in a timely manner.

Approvals shall be granted to the licensee after receipt of the request and after fulfilment of the regulatory requirements. Upon the result of its assessment, the Regulatory Authority may or may not grant the authorization requested. In the event of failure to comply with the requirements for approval, the licensee shall be notified in writing of the Regulatory Authority's decision.

CHAPTER IV: SECURITY ASSESSEMENT AND AUDIT OF NETWORKS AND SYSTEMS OF LICENSEES

Article 20: Security Assessment of all Planes

The licensee shall perform on annual basis, a vulnerability assessment and penetration testing of all planes to identify the weaknesses and fix them in a timely manner.

Such assessment shall be conducted by an external and independent party and the report must be shared with the Regulatory Authority as soon as it is available.

Article 21: Vulnerability Assessment

To conduct the vulnerability assessment of their network and systems, the licensee must:

(a) have test devices, nodes and applications with manual or automated tools;
(b) conduct vulnerability assessment on all planes;
(c) perform security testing prior to granting approval for systems to move into production;
(d) fix the identified vulnerabilities by applying patches 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

The licensee shall on annual basis, conduct an independent security and compliance audit to verify the effectiveness of the implemented security controls such as management, technical

and physical controls. Such audit must also be conducted immediately after a critical/major incident or following a system upgrade.

The Licensee shall measure the effectiveness of implemented controls and, on any controls' shortfall or failure, the licensee must implement the remediation plan as soon as possible**.**

Depending on the nature of the audit findings, the remediation plan may be extended but not exceed three (3) months as may be determined by the Regulatory Authority.

Article 23: Compensatory Controls

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

Article 24: Mitigation of Risks Leading to Subscribers' Loss of Service

The licensee shall put in place documented security policies and procedures to mitigate all known risks associated with the services offered to avoid damage to, or failure of systems, which may cause interruptions of subscribers' services or make subscribers suffer from any associated losses.

Article 25: Submission of the Security Assessment and Audit Reports

The licensee shall submit security assessment reports, audit plans and audit reports to the Regulatory Authority not later than thirty (30) calendar days after completion of the assessment and audit.

Article 26: Remediation Plan

The licensee shall submit the remediation plan to the Regulatory Authority along with the audit reports.

Article 27: Regulatory Authority Audit

The licensee shall comply with this regulation and the Regulatory Authority shall conduct audit on annual basis or at a time when need arises. All network and system vulnerabilities identified

shall be communicated to the licensee for remediation. The remediation plan shall be submitted to the regulatory Authority not later than 30 days after the audit report.

The licensee is required to facilitate the auditors by providing requested information and evidence.

The Regulatory Authority shall issue notification to the licensee two (2) weeks prior to conducting the regulatory security audit.

CHAPTER V: EFFECTIVE MANAGEMENT OF INCIDENTS

Article 28: Incident Management

The Licensee must protect their networks and systems, which include but is not limited to:

(a) implementation of a security incident reporting and handling process;
(b) incident management process and training of employees on incident handling processes and procedures;
(c) guidelines for identifying a security incident;
(d) communication channels to be used for reporting the security incident;
(e) recording security incidents reported;
(f) assigning severity to security incidents;
(g) escalation mechanism for security incidents;
(h) resolution and closure of incidents;
(i) root cause analysis leading to process improvements;
(j) monthly report to business for root cause analysis; and
(k) creating an internal incident management team to work in cooperation with government Computer Security Incident Response Team (CSIRT) to effectively handle security incidents.

The categorization of incidents under this provision is contained in ***ANNEX I*** of this Regulation.

Article 29: Sharing Information on Security Incident

The licensee and/or any service provider interfacing with the licensee shall immediately share with the Regulatory Authority information on any security incidents which have occurred and considered as critical or major as defined in ***ANNEX I*** of this Regulation. Such information

will be shared within 24 hours of the incident(s) occurrence through E-mail specified by the Regulatory Authority.

Initial notification of "urgent incidents" shall be made by the licensee within three (3) hours of incident occurrence, through E-mail specified by the Regulatory Authority.

The licensee must submit reports of moderate and minor incidents on a monthly basis through electronic communication channels prescribed by the Regulatory Authority.

The Regulatory Authority shall be shall be notified of all incidents using the incident report form as contained in ***ANNEX II*** of this regulation.

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

Article 30: Monitoring and Compliance

The licensee shall monitor and comply with all security standards provided for under this regulation to maintain secured networks, systems and services.

The Regulatory Authority shall conduct audits for compliance with this Regulation on annual basis or at a time when need arises.

Article 31: Reporting

All assessments, audit plans and reports shall be submitted to the Regulatory Authority in the prescribed manner within the time limit specified in this regulation.

The regulatory authority may at any time determine the audit format and communication channel through which security incidents will be reported by the licensee.

CHAPTER VI: ADMINISTRATIVE SANCTIONS

Article 32: Non-Compliance with the Network and Systems Security Enforcement Notice

Any 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 one million (1,000,000) and five million (5,000,000) Rwandan francs.

Failure to comply with the enforcement notice shall incur an additional administrative fine of five hundred thousand (500,000) Rwandan francs per day as calculated from the date of receipt of the concerned enforcement notice.

Article 33: Failure to Implement Security Measures

Any licensee who fails to implement the relevant security measures to avoid interruption of subscribers' services shall be liable to an administrative fine between one million (1,000,000) and five million (5,000,000) Rwandan francs.

Continuous failure to implement the security measures shall incur additional sanctions that may lead to revocation of the license.

Article 34: Refusal to Provide Information Related to Security Incidents

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

Article 35: Delay to Submit the Reports

Any licensee who intentionally or by negligence fails to submit the audit plan, 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) Rwandan francs.

Article 36: Non-Compliance with any Requirement of this Regulation

Any 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) Rwandan francs.

Article 37: Additional Sanctions

The Regulatory Authority reserves the power to impose additional sanctions in accordance with applicable laws and regulations when deemed necessary.

CHAPTER VII: FINAL PROVISIONS

Article 38: Repealing Provision

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

Article 39: 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 29/05/2020.

Dr Ignace GATARE

Chairperson of the Regulatory Board

ANNEX I: CATEGORIZATION OF INCIDENTS

	Core Services	**Value-Added Services (VAS)**
Entire Network	**Urgent**	Critical
Partial Network	Critical	Major
Subscriber	Moderate	Minor

ANNEX II: SECURITY INCIDENT REPORT FORM

The following is a sample incident report form. The report is an example of the types of information and incident details that will be used to track and report security incidents to the Regulatory Authority.				
Contact Information				
1.	**Company Name**			
2.	**Last Name**		**First Name**	
3.	**Job Title**		**Mobile No**	
4.	**Email:**			
Incident General Information				
5.	**Type/Name of Incident**			
6.	**Brief description of incident**			
7.	**Date/Time of Incident Detection/Occurrence**		**Time:**	**Date:**
8.	**Site/Location**			
9.	**Date and time of Resolution**			
10.	**Known Impact**			
11.	**Confidential/Personal Identifiable Information Affected**		☐ **Yes** ☐ **No**	
12.	**Systems and Services Impacted**		**Service(s) affected**	
			Number/proportion of users affected	
			Networks & assets affected	
13.	**Severity Level**		**Critical** ☐	**Major** ☐
			Moderate ☐	**Minor** ☐
14.	**Summary of incident cause and action taken so far**			
15.	**Source of Incident**		**Description:**	
			Internal ☐	**External** ☐
16.	**Third party details [*If the cause of the incident was the failure of a third-party service]***			
17.	**Name and contact details for follow up *[If different from above*]**			
18.				

Incident Mitigation	
Status	
Timeline	
Comments	
Additional Comments/Notes/Recommendation	
[Any additional notes, Follow-on actions recommended to be taken, information or observations related to the security incident or this report]	

Seen to be attached to the Cybersecurity Regulation N° 010/R/CR-CSI/RURA/020 of 29/05/2020.

Dr Ignace GATARE

Chairperson of the Regulatory Board