National Cyber Security Policy

March 2015

ACRONYMS

Acronym	Expansion
AMIS	Agriculture Management Information System
CCIP	Centre for Critical Infrastructure Protection
CIIs	Critical Information Infrastructures
CMU	Carnegie Mellon University
CS	Cyber Security
CSIRT/CERT	Computer Emergency and Security Incident Response Team
CSOC	Cyber Security Operations Centre
DDos	Distributed Denial of Service
EA	Enterprise Architecture
EDPRS	Economic Development & Poverty Reduction Strategy
EU	European Union
e-GOV	E-Government
FDI	Foreign Direct Investment
G2B	Government to Business
G2C	Government to Customer
G2G	Government to Government
GDP	Gross Domestic Product
GEA	Government Enterprise Architecture
GoR	Government of Rwanda
GSA	Government Security Architecture
HMIS	Hospital Management Information System
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
IOS	International Organization for Standardization
IT	Information Technology
IaaS	Infrastructure as a Service
ITSD	Information Technology Services Division or Directorate
KIST	Kigali Institute of Science and Technology
KLab	Knowledge Lab
MOD	Ministry of Defense
MYICT	Ministry of Youth and ICT
NCSSP	National Cyber Security Strategic Plan

NICI	National Information and Communication Infrastructure
NID	National ID
NISS	National Intelligence and Security Services
NIST	National Institute of Standard and Technology
NSRC	National Cyber Security Research Center
OCS	Office of Cyber Security
Open EMR	Open Electronic Medical Record
PaaS	Platform as a Service
PDF	Portable Document Format
PIKE	Predominantly Information and Knowledge-based Economy
PKI	Public key Infrastructure
PM	Project Manager
PMR	Professional Mobile Radio
PSCBS	Public Sector Capacity Building Secretariat
RDB	Rwanda Development Board
RRA	Rwanda Revenue Authority
RURA	Rwanda Utilities Regulatory Authority
SaaS	Software as a Service
SOC	Security Operation Center
TETRA	Terrestrial Trunked Radio
WDA	Workforce Development Authority

TABLE OF CONTENTS

FOREWORD

The Government of Rwanda (GoR) has invested significantly in Information and Communications Technology (ICT) infrastructure and applications, as a cornerstone for National economic growth. ICT is recognized as a key enabler for economic growth and social mobility and is expected to improve Rwandans' standard of living as part of the Integrated ICT-led Socio-Economic Development Policy and Plan.

Even though the rapid development of ICT in Rwanda promises a positive impact on the nation's economic growth, these technologies have introduced new types of threats such as cyber-crime, cyber espionage, Hacktivism, Cyber Terrorism, Cyber Warfare, to mention a few. Cyber threats are on rise globally and are proving increasingly sophisticated, and difficult to mitigate; the imminent threat of cyber-crime to National Security means that GoR must be prepared and in the position to prevent and respond to evolving cyber threats.

Given the heavy investment in the ICT infrastructure to support its economic development goals, it is imperative that infrastructure be resilient and secure against cyber threats. The first National Cyber Security Policy for Rwanda to establish an environment that shall assure the trust and confidence while using ICT facilities and ensure that Rwanda is self-reliantly able to protect its interests and enforce national security. This policy will guarantee the confidentiality and integrity of information assets and sensitive information of Government, Businesses and individuals.

The Ministry in charge of ICT in collaboration with key stakeholders in Cyber security especially Rwanda Development Board, Ministry of Defense, Ministry of Internal Affaires, Rwanda National Police, took a lead in the development of cyber security policy, and will periodically review its implementation progress to ensure that threats of current and potential cyber-attacks are addressed in a timely and appropriate manner.

1. ISSUE

The growth of the Internet has been the biggest social and technological change in recent timesreduces barriers to trade, and is playing a huge role in supporting sustainable development in Rwanda.

Increasing use of the Internet and other digital technologies increases our vulnerability to cyber threats, increasing dependence on cyberspace has brought new risks, Criminals are increasingly using cyber space to gain access to personal information, steal businesses' intellectual property, and gain knowledge of sensitive government-held information for financial or political gain or other malicious.

1.1. INTRODUCTION

The government of Rwanda has embarked on developing a cyber security policy and strategy as response to the growing cyber threat and improving cyber security for individuals, businesses, critical national infrastructure and government.

1.2. CONTEXT

Given the vision to become a middle-income, knowledge-based economy, it is imperative that great importance be attached to the efficient handling of knowledge and information.

Rwanda's goal to be a regional ICT Hub, and considering current ICT industry growth trends, has made Cyber security a compelling priority for Rwanda. Cyber Security was identified as a key priority for the third phase of NICI, in order to ensure secure management of all deployed ICT assets that support Rwanda's ICT goals.

The cyber security policy for Rwanda shall create a framework for defining and guiding the actions related to security of cyber space. The policy framework should provide the foundation required to ensure that initiatives by public and private sectors continue to enjoy consistent and undiminished support throughout the coming years, up to realization of the visions encompassed in the afore-mentioned strategy documents.

The cyber security policy is developed in line with national, regional and international recommendations on cyber security, including but not limited to, International Telecommunication Union (ITU), Africa Union (AU) and East Africa Community (EAC) recommendations.

1.3. BACKGROUND

The Government of Rwanda (GoR) recognizes the potential of ICT as a crosscutting enabler for all development sectors, and thus holds potential to improve Rwandan standards of living. GoR has set the tone for development and investment within the ICT sector by putting in place strategic plans and agendas at sector and national level.

The GoR has a strong public policy towards the development of country, utilizing ICT as one the crosscutting enablers:

- **Vision 2020** establishes a goal to move Rwanda from an agrarian economy to information-rich, service-oriented, knowledge-based economy by 2020.

- **The Economic Development and Poverty Reduction Strategy (EDPRS)** seeks to drive speedy yet sustainable economi c growth and outlines the role of ICT in leapfrogging key stages of industrialization in order to achieve national economic objectives.

- **The National ICT and Strategy Plan (NICI)** outline a four-phase approach to achieving Vision 2020 through ICT. Phase I (2000-2005) focused on the creation of an enabling institutional, legal and regulatory environment for ICT development; Phase II (NICI I-2010) concentrated on development of critical national ICT infrastructure; Phase III (National ICT strategy and plan 2011-1015) focuses on leveraging the existing infrastructure and environment to improve service delivery as well as enhance cyber security for Rwanda.

In light of this, there has been significant investment in ICT infrastructure and applications considered as critical information assets for Rwanda. As a result, there is increasing dependency on the proper functioning and operation of ICT infrastructure in all sectors. This includes, but is not limited to, reliance on the Internet for e-Government, commercial operations such e-Commerce, e-Banking and other ICT-based services.

In addition, the Rwandan society has become increasingly dependent on ICT for business, health, education, agriculture, and other sectors. The protection and availability of these critical assets are paramount and as such, cyber security has become a strategic national issue affecting all levels of our society.

Enhancing cyber security and protecting critical information infrastructures is essential to national security and economic wellbeing. Securing Rwandan cyberspace requires comprehensive, collaborative and collective efforts to deal with cyber security at all levels

and this requires an appropriate and comprehensive cyber-security policy framework to ensure the security and resilience of national information systems and services.

1.4. CURRENT STATUS OF CYBER SECURITY

Rwanda is aware that cyber security threats are posing a global danger to the integrity, security and privacy of information worldwide, and that in the twenty-first century every country shall have to protect its cyber-space in order to protect its citizens.

Although there have been significant investments and government interventions to address cyber security challenges through various institutions, there is a need for a strong institutional framework to coordinate cyber security initiatives with an integrated approach as to fully realize cyber security strategic objectives. The absence of such an institutional framework has often led to inconsistency and duplication of efforts among stakeholders.

In terms of Policy, Legal, and Regulatory Framework and Standards governing ICT, addresses issues related to ICT Services and Security. This includes ICT Policy and regulatory functions, consumer protection, matters of national interest and data security, regulation of electronic certification service providers, obligations of certification authorities (CAs), computer misuse, cyber-crime, and protection of personal information.

The comprehensive ICT law under final review for enactment shall supersede several ICT related laws including “Law relating to electronic messages, electronic signatures and electronic transactions”. Even though the penal code and the current ICT bill outline provisions for cyber security, there are still gaps such as no legal basis and procedures for designating and managing the critical information infrastructures (CIIs) and no adopted national cyber security standard in Rwanda, resulting in inconsistency of security policies in each organization. In an effort to enhance the cyber security regulations,

Several infrastructure and initiatives have been implemented in cyber security which include the establishment of an Internet Security Center (ISC) to monitor the status of Internet security, and the National Public Key Infrastructure (PKI) to provide confidentiality, integrity, authenticity and non-repudiation of e-Transactions, establishment of a National Computer Security and Incident Response Team (CSIRT), mandated with preventing and responding to cyber security incidents in public and private cyberspace.

All the above would protect critical infrastructure such as the National Backbone (NBB), National Data Center (NDC), 4G LTE last mile networks, e-Government systems, Energy Infrastructure, Banking and Finance systems, etcetera. This infrastructure needs to be highly protected both logically and physically.

There have been several Cyber Security Capacity Building initiatives, to improve Rwandan cyber-security capabilities including the development and implementation of education and training programs in cyber and information security; collaboration and partnership with international cyber security agencies to ensure knowledge and skills transfer; and training programs for trainers. Although these initiatives are remarkable, there are still areas that require more and improved skills in order to meet the needs of all public and private sector stakeholders. It is also important to establish a cyber-security culture and increase awareness among citizens.

1.5. PRINCIPLES

In order to align strategic objectives with current government efforts and the international community, the development of the National Cyber Security Policy of Rwanda followed these fundamental principles:

- **National Leadership** – The scale and complexity of cyber security requires strong national leadership;
- **Roles & Responsibilities** – All ICT users including government, businesses and citizenry should take reasonable steps to secure their own information and information systems, and have an obligation to respect the information and systems of other users;
- **Public-Private Collaboration** – A collaborative approach to cyber security across government and the private sector is essential and crucial;
- **Risk-Based Management** – There is no such thing as absolute cyber security. Rwanda must therefore apply a risk-based approach to assessing, prioritizing and resourcing cyber security activities; to be revised as among other based
- **Rwandan Values** – Rwanda pursues cyber security policies that protect the society, the economy and the national vision;
- **International Cooperation** – The cross-border nature of threats makes it essential to promote international cooperation. Rwanda supports and actively contributes to the international cyber security activity.

2. THE NATIONAL CYBER SECURITY POLICY

2.1. MISSION

The mission of the National Cyber Security Policy is "to ensure Rwandan Cyber Space is secure and resilient"

2.2. STRATEGIC OBJECTIVES

The goals and objectives of the National Cyber Security Policy are as follows:

- Build cyber security capabilities for detection, prevention and response to cyber security incidents and threats;
- Establish an institutional framework to foster cyber-security governance and coordination;
- Strengthen legal and regulatory frameworks, as well as promote compliance with appropriate technical and operational security standards,
- Promote Research and Development in the field of cyber security;
- Promote Cyber Security Awareness in all sectors and at levels in order to build a culture of security within country;
- Promote National, Regional and International Cooperation in the field of cyber security.

2.3. KEY POLICY AREAS

POLICY AREA 1 – CYBER SECURITY CAPABILITIES

Objective: To build cyber security capabilities to manage Cyber Security incidents and respond promptly to cyber threats.

Measures:

1) National Computer Security and Incident Response Team

The established Computer Security and Response Center shall be officially approved as a National Computer Security and Incident Response referred as "Rw-CSIRT". The Rw-CSIRT

shall be strengthened to detect, prevent and respond to cyber security threats and will play a coordination role of incidents response. Providing human resources as well as adequate capacity building resources will strengthen the National CSIRT operation capabilities.

2) Develop National Cyber Contingency Plan

A National Cyber Security Contingency Plan (NCCP) shall be put in place to provide measures for responding to and recovering after major incidents that involve Critical Information Infrastructure (CII). NCCP shall outline the criteria to be used to identify a crisis, define key processes and actions for handling the crisis, and clearly define the roles and responsibilities of different stakeholders during a cyber-security crisis.

3) Establish Cyber Security Capabilities within institutions

Depending on the size and complexity of information technology infrastructure and systems, public and private organizations shall establish a cyber security function within the IT units, responsible for planning and implementing cyber security programs.

POLICY AREA 2 – INSTITUTIONAL FRAMEWORK FOR CYBER SECURITY

Objective: To build cyber security capabilities and secure national information assets requires a sound governance structure for effective coordination of national cyber security initiatives.

Measures:

4) Establish an Agency in charge of National Cyber Security

Given the complexity of the cyber security threats to the overall national security, there is a need for a strong institutional framework to coordinate cyber security initiatives with an integrated approach as to fully realize cyber security strategic objectives. The absence of such an institutional framework has often led to inconsistency and duplication of efforts among stakeholders.

Therefore, the GoR shall establish an Agency in charge of National Cyber Security responsible for the development, implementation and coordination of the national cyber security initiatives.

5) Establish a National Cyber Security Advisory Board

In order to establish strong cyber-security governance framework, the GoR shall put in place a National Cyber Security Advisory Board (NCSAB). This board shall provide strategic guidance on matters related to cyber security. The composition of the Board should consider public and private organs relevant to cyber security.

POLICY AREA 3 – CYBER SECURITY LEGAL AND REGULATORY FRAMEWORK

Objective: To strengthen the existing legal and regulatory framework so as to comprehensively address cyber-crime and facilitate the criminalization of acts related to cyber-crime that are not addressed by any existing law, yet pose a potent threat to national security.

Measures:

6) Enhance the legal and regulatory framework

There is a need to enhance the current legal and regulatory framework to facilitate the enforcement of cyber security laws, investigation and prosecution of cyber-crime related activities.

To this end, the GoR shall review the existing legal and regulatory framework to ensure that all applicable national legislations incorporate cyber security provisions that grant reasonable capacity to national law enforcement agencies, which are complementary to, and in harmony with, international laws, treaties and conventions.

The GoR will also strengthen the legal and regulatory framework to prevent cyber security threats arising from harmful content disseminated in the national cyberspace.

7) Define Standards and Guidelines

To ensure information security best practices with public and private institutions, the agency in charge of cyber security shall develop standards and guidelines to guide public and private sector players adopt consistent cyber security best practices and standards.

POLICY AREA 4 – CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

Objective: To protect National Critical Information Infrastructure against cyber threats and related cyber-crimes to ensure its confidentiality, integrity and availability.

Measures:

8) Protect National Critical Information Infrastructure

The disruption of Critical Information Infrastructures (CIIs) has direct impact on business and society. Therefore, the Government institution in charge of cyber security shall put in

place a mechanism to ensure that National Critical Information Infrastructure (CII) is defined and secure against various cyber threats.

In collaboration with the ICT Regulatory Authority, the concerned public institutions as well as the private sector relevant to cyber security shall develop the CII Information Protection law, CII regulations, compliance and compliance and protection plan. CII regulation shall address, but shall not be limited to, CII procedures manuals, access control, business continuity and contingency plan, physical and logical protection.

9) Establish Public-Private Collaboration Framework

Given the role that the private sector plays in the development and management of ICT infrastructure and services, collaboration with the private sector is key in addressing security and resilience. The Agency in charge of Cyber Security shall put in place a collaboration framework that defines the roles and responsibilities of organizations managing critical Information Infrastructure.

The GoR and Private Sector will meet regularly to discuss and review the security status of CIIs and share cyber security related information.

POLICY AREA 5 – GOVERNMENT CYBER SECURITY ENHANCEMENT PROGRAM

Objective: To safeguard Government information and infrastructure systems against cyber-attacks.

Measures:

10) Information Security Compliance

The Agency in charge of Cyber Security shall establish the Government Information Security Certification (GISC) program based on Government Security Architecture (GSA) to enhance Information Security Management System in public institutions. The agency in charge of cyber security shall conduct an information security audit in public institutions based on GSA requirements. Private institutions are also subject to a mandatory information security audit at least once a year based on ISO 27001/27002 or GSA, in case required they shall seek support from the agency in charge of cyber security.

11) Establish security levels for systems, applications and services,

The Agency in charge of Cyber Security shall define security levels of systems, applications and services for GoR. More especially, e-Government services must adopt appropriate cyber

security technology and improve their overall security capability. The security level of e-Government services shall be based on the risk-based assessment.

12) Establish secure and reliable environment for e-Government and e-commerce with National Public Key Infrastructure

The GoR shall promote the use of national Public Key Infrastructure (PKI) in order to establish a secure and reliable environment for e-Government and e-Commerce through security services based on PKI technology including authentication, data integrity, confidentiality, and non-repudiation

In collaboration with other stakeholders, the ICT Regulator shall put in place laws, regulations, policies and standards that promote use of national PKI.

The ICT regulatory Authority shall manage the Root Certification Authority (Root CA) and licensing of PKI services and shall define the requirements for Accredited Certification Authority (ACA) and usage of digital certificate.

The Agency in charge of Cyber Security shall be accredited as the GoR certification authority. In collaboration with other certification Authorities, it shall promote the usage of digital certificates in critical e-Government services, e-Commerce, e-Banking, e-Healthcare system as well as other sectors.

POLICY AREA 6 – CYBER SECURITY CAPACITY BUILDING AND AWARENESS

Objectives: (i) To build cyber security prevention and response capabilities; (ii) To create cyber security awareness for the Rwandan citizens.

Measures:

13) Cyber Security Capacity Development

Cyber security threats are dynamic and complex to mitigate and require a comprehensive program of continuous development of human capacity and retention policy.

To ensure a sufficient level of expertise in the field of cyber security across the public and private sector, the Agency in charge of Cyber Security shall develop and implement a cyber-security capacity-building program. In this program a workforce of professionals skilled in cyber security shall be crated through capacity building, skills development and professional training.

14) Develop a National Cyber Security Awareness Program

It is important that citizens in Rwanda using or operating information assets understand the threats and risks in cyber space. The Agency in charge of Cyber Security shall develop a cyber-security awareness program for institutions and individuals as well as encourage ownership.

POLICY AREA 7 – BUILDING A CYBER SECURITY INDUSTRY

Objective: Develop a stronger cyber security industry to ensure a resilient cyber space.

Measures:

15) Foster innovation through Research and Development

In cooperation with the academia and industry, a Cyber Security Research and Development (R&D) program shall be developed. The Research and Development program shall focus on the development of intelligent intrusion prevention and detection systems, Forensics, encryption and mobile security. In a bid to nurture the growth of cyber security industry, the products and services resulting from cyber security innovations shall be commercialized within and outside Rwanda.

The R&D programs shall also address aspects related to development of security trustworthy technology systems and solutions, security evaluation of emerging technologies and devices, and research on emerging cyber threats.**16) Promote and strengthen the private sector participation in Rwanda's cyber security industry development.**

To develop a stronger cyber security sector or industry, a public private partnership shall be established to develop cyber security services, skills and expertise that respond to cyber security objectives. This will position Rwanda as a regional hub that exports services and skills in the cyber security field.

POLICY AREA 8 – INTERNATIONAL COOPERATION

Objective: To establish a regional and international cooperation framework to protect national Cyber space.

Measures:

17) Promote and strengthen Regional and International collaboration

Engaging in cooperation and information sharing with partners abroad is important to better understand and respond to a constantly changing threat environment. International investigations depend on reliable means of cooperation and effective harmonization of laws.
The Agency in charge of Cyber Security shall continually enhance international cooperation in cyber law and in response to cyber threats. The Agency will support and participate in international research projects and the exchange of experts in cyber security to enhance cyber security capabilities.

3. INSTITUTIONAL FRAMEWORK

3.1. PROPOSED INSTITUTIONAL FRAMEWORK FOR IMPLEMENTATION

Securing Rwanda's national information assets requires an adequate and comprehensive governance structure for effective focus and coordination of national cyber security initiatives. It is necessary therefore to establish an efficient coordination mechanism for effective cyber security and resilience.

The cyber-security implementation framework is composed of the National Cyber Security Advisory Board, the Agency in charge of National Cyber Security, supported by ICT units within public and private sector institutional.

3.2. INSTITUTIONAL ROLES

The section below describes the roles and responsibilities of organs involved in the implementation of this policy.

THE NATIONAL CYBER SECURITY ADVISORY BOARD (NCSAB)

The National Cyber Security Advisory Board will be created as part of the cyber security agency, which provides strategic, and leadership, oversight and guidance on implementation and development of national cyber security initiatives.

THE AGENCY IN CHARGE OF CYBER SECURITY

The Agency in charge of National Cyber Security is responsible for planning, coordination and implementation of national cyber security initiatives. It ensures institutional conformance to information security standards, guidelines and best practices necessary to secure Rwanda's cyber space. It shall conduct cyber security audits, assessments and readiness exercises for government institutions and develop standards and best practices for Rwanda as a whole; it

shall conduct research on cyber security policy, legal and technical issues, support awareness campaigns and provide cyber-security training programs.

The Agency operates and maintains national cyber security infrastructure and systems and provides technical support to institutional cyber-security units. It is responsible for developing necessary expertise and conducting research and development in cyber security. It promotes national awareness and coordinates cyber-security workforce development. Furthermore, it represents Rwanda in international forums on issues of cyber security.

The Agency will coordinate and support Government Ministries, Agencies and Private sector institutions to develop cyber security capabilities and implement this policy.

4. FINANCIAL AND LEGAL IMPLICATIONS

4.1. FINANCIAL IMPLICATIONS

The proposed National Cyber Security Policy define different initiatives that will require financial resources, such as the establishment and operationalization of the suggested National Cyber Security Agency (NCSA) that will spearhead the implementation of this policy. The agency will define the short and long-term strategic plan and budget, which will be considered during the next budget revision.

4.2. LEGAL IMPLICATIONS

The approval of this policy will require Act of parliament establishing cyber security agency as public organisation, defining its mandate and functions as well as transferring the cyber security responsibilities from RDB to the agency in charge of cyber security.

It will be followed by the review of existing legal framework to ensure that all applicable national legislations incorporate cyber security provisions, which will follow the normal law reform process and procedure as well as consultations.