REPUBLIC OF RWANDA

National Cyber Security Strategic Plan

Kigali, March 2015

1. Objective

This document aims to provide an implementation guidance of the defined National Cyber Security Policy (NCSP). Specifically it defines the establishment of a National cyber security Agency, new cyber security initiatives and priorities, roles and responsibilities for parties who will be involved in the implementation and financial implication.

2. National Cyber Security Institution Framework

The NCSP define the establishment of a strong and effective cyber security Governance in the country which provide a strong leadership in the area of National Cyber Security and information security programs. This framework defines the establishment of National Cyber Security Advisory Board (NCSA), National Cyber Security Agency (NCSA), public and private institutional ICT units with cyber security functions as well as specialized cyber security centers.

The figure bellow illustrates the Cyber Security Institution Framework.

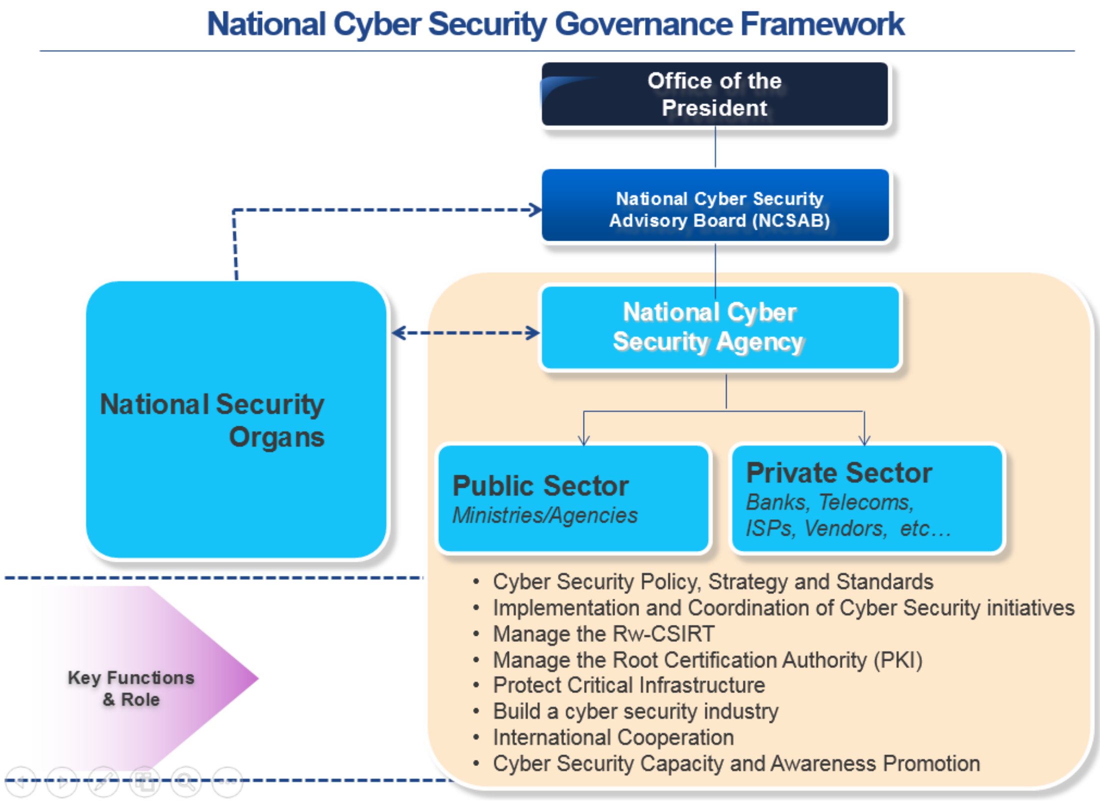

National Cyber Security Governance Framework
Office of the President
National Cyber Security Advisory Board (NCSAB)
National Security Organs
National Cyber Security Agency
Public Sector
Ministries/Agencies
Private Sector
Banks, Telecoms, ISPs, Vendors, etc…
Key Functions & Role
• Cyber Security Policy, Strategy and Standards
• Implementation and Coordination of Cyber Security initiatives
• Manage the Rw-CSIRT
• Manage the Root Certification Authority (PKI)
• Protect Critical Infrastructure
• Build a cyber security industry
• International Cooperation
• Cyber Security Capacity and Awareness Promotion

Figure 1: Cyber Security Institution Framework

2.1. The National Cyber Security Advisory Board (NCSAB)

A National Cyber Security Advisory Board (NCSAB) will be established in order to provide a strategic leadership, oversight and guidance on implementation and development of national cyber security programs. Specifically the NCSAB will play an advisory role to the National Cyber Security Agency. The NCSAB will be composed by the heads of National Cyber Security Organs, relevant line Ministries and representatives from the private sector.

2.2. National Cyber Security Agency (NCSA)

The NCSP define the establishment of a National Cyber Security Agency in charge of cyber security, mainly that will spearhead the implementation of the National Cyber Security policies and strategies. The NCSA will lead the implementation of this plan to ensure that Rwandan Cyber Space is secure and resilient against cyber threats. In striving to achieve this, the NCSA will:

- Ensure Planning, coordination and implementation of national cyber security policy/strategy and other related information security initiatives;
- Put in place strategies to build a sustainable cyber-security industry to position Rwanda as a regional hub.
- Protection of National Critical Information Infrastructure (CII) and Information Systems as well as the non-critical.
- Information security assessment of public and private networks, systems and applications to ensure compliance with best practices.
- Ensure appropriate legal and regulatory frameworks are in compliance with national and international cyber security standards and best practices.
- Promote education and professional training to ensure the development of skilled workforce in the area of cyber security
- Promote Cyber Security Awareness in all sectors and at levels in order to build a cyber security culture and cyber aware society;
- Support the establishment of cyber security capabilities within public and private institutions and sector CERTs.

- Promote National, Regional and International Cooperation, Research and Development in the field of cyber security.

To achieve its mission and objectives, initially the NCSA will be composed of four major departments that will focus on the development and implementation of cyber security priorities and programs defined in the NCSP, below is a brief description of the roles and responsibility of each department.

1. **National Computer Security and Incident Response Team (Rw-CSIRT)**: The Rw-CSIRT will operate under the auspice of the NCSA, it will act as a national point of contact for the coordination of incident handling activities. Specifically the National CSIRT will provide 24/7 services to Detect, Identify, Analyze, Prevent and Response to cyber security threats and computer security incidents.

2. **Information Certification Department**; The Information Certification Department will act as National Information Certification Center, it will manage National PKI facilities, issue and revoke digital certificates to users, entities and systems. This department will focus on securing electronic transaction and communication, especially to ensure usage of e-Government and e-commerce service are used in a secure. In collaboration with the regulator of PKI this department will develop PKI Policy, Standards and promote PKI usage.
3. **IT Security Audit and Compliance Department**: The IT security Audit and Compliance Department will be responsible to assess and evaluate the security posture within public and private organizations. Based on the developed Government Security Architecture (GSA) and International Security Standards (ISO27001/27002), the department will carry out rigorous Information security audit including risk analysis, vulnerability assessment and Penetration testing and will certify Ministries and Agencies in compliance with defined information security standards and best practices. The department will also develops standards and best practices for Rwanda.

4. **Cyber Security Development and Operation Department**; The CS Development and Operation Department will be responsible for promoting research and development in the field of cyber security focusing in the development of new security solutions and systems technology to mitigate cyber threats. It also focus on developing and implementing cyber security workforce program.

2.3. National Cyber Crime Investigation Center (NCCIC)

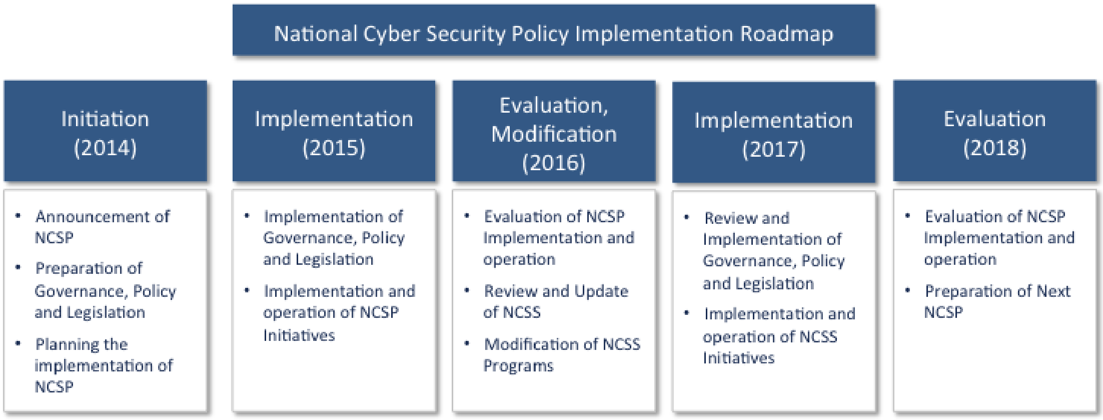
Considering the increasing number of cyber crimes, there is a need to establish a National Cyber Crime and Investigation Centers, this center will focus on building the national capability to investigates cyber crimes, retrieve and analyze digital evidence from different digital media (e.g. Computers, Network, Wireless network, smart phones and other portable digital media, etc.…)

2.4. NCSP Implementers

Once the Cyber Security Agency is established, it will support concerned Ministries and Government Agencies to implement this policy. These institutions include: The Ministry of Defense (MOD), Ministry of Internal Security (MININTER), Ministry of Youth & ICT (MYICT), Ministry of Finance & Economic Planning (MINECOFIN), Ministry of Justice (MINIJUST), Rwanda National Police (RNP), National Intelligence and Security Services (NISS), Rwanda Development Board (RDB), Rwanda Utilities Regulatory Authority (RURA), Agency in charge of ICT and the Private sector among others.

3. NCSP Implementation framework

The NCSA will be the leading organization to plan the implementation, monitoring and evaluation of cyber-security programs set to commence upon approval of this policy by the Cabinet. For effective implementation, this policy will be regularly reviewed annually to evaluate the implementation progress. The table defines brief implementation plans of National Cyber Security Policy.



National Cyber Security Policy Implementation Roadmap

Initiation (2014)	Implementation (2015)	Evaluation, Modification (2016)	Implementation (2017)	Evaluation (2018)
• Announcement of NCSP • Preparation of Governance, Policy and Legislation • Planning the implementation of NCSP	• Implementation of Governance, Policy and Legislation • Implementation and operation of NCSP Initiatives	• Evaluation of NCSP Implementation and operation • Review and Update of NCSS • Modification of NCSS Programs	• Review and Implementation of Governance, Policy and Legislation • Implementation and operation of NCSS Initiatives	• Evaluation of NCSP Implementation and operation • Preparation of Next NCSP

4. Implementation plan and Financial Implication

The proposed policy defines the establishment of a National Cyber Security Agency and implementation of new projects, which involves financial implication. The table bellow defines new projects, project activities, responsible institutions, implementation schedule and estimate cost for each project.

The time schedule of this policy has been based on the assumption that the preparation for the implementation will start immediately upon approval of the policy by the cabinet.

Table 1: Strategic Plan 2015 - 2020

Deliverable	Next Activities	Start Date	End date	Responsible	Estimated cost (FRW)
Establish a National Cyber-Security Agency Council.	• Draft legal framework to establish a NCSA, Mandates and organization structure • Appoint members of the National Cyber Security Council Operational strategic plan for the Agency • Operationalize the cyber security agency	May 2015	August 2015	RDB MYICT MoD RNP	1,200,000,000 x 5 Years
Cyber Security Legal and Regulation Framework	• Establish a task force to review cyber security legal and Regulatory frameworks • Revise legal and regulatory framework to harmonize and comply with international laws, treaties and conventions • Improve and strengthen mechanisms for law enforcement vis-à-vis cyber security • To strengthen the legal and regulatory framework related to online child protection, personal data privacy protection, and promotion of better use of online contents disseminated through electronic and social media.	January 2015 (*Ongoing activity*)	June 2015	MINIJUST MYICT RURA RNP	200,000,000
National Cyber Contingency Plans (NCCPs)	• Define processes, procedures and measures for crisis handling and data recovery	June 2015	September 2015	MYICT, NCSA,RURA MoD RDB RNP	150,000,000
Enhance the capacity of established Rw-CSIRT	• Recruit additional staff and provide advanced security professional training to • Advance and Expand services provided by the National CSIRT • Establish a National Alert and Warning System • Establish a Unified Security Management System across public institutions	April 2015	April 2017	MYICT RDB	1,500,000,000

National Cyber Crime and Investigation Center.	• Develop legal digital forensics framework (i.e. Legal processes and Policies) • Capacity building for digital forensics expert and legal enforcement • Define the Mission, Roles & Responsibilities, Organizational structure and Operational policy for National digital forensics center • Design and implement National Cyber Crime and Forensics Center facilities (i.e. Building, Hardware and Systems)	June 2017	June 2018	MYICT RNP RDB	3,500,000,000
Critical Information Infrastructure Protection CIIs	• Establish CIIP Joint Committee from the Public and Private sector • Identify and Protect CIIs • Draft legal framework for the protection of Critical Information Infrastructure Protection Act • Develop the Policy, procedures and Guidelines to assess, manage and review CIIs	June 2016	June 2017	NCSA RDB ISPs and other Private players	250,000,000
Public-Private Collaboration Framework	• Establish a task to study and define the framework • Develop public-private partnership framework on cyber security • Establish a trusted information sharing mechanism	April 2015	August 2015	MYICT RURA RDB ISPs and other Private players	30,000,000
Establishing a secure and reliable environment for e-Government and e-commerce with PKI	• Develop a National Public Key Infrastructure (PKI) Policy • Establish an Accredited Certification Authority that issues digital certificates to Entities, Individuals and Devices • Define the regulations to regulate usage of digital signature in e-Government and e-commerce • Raise awareness of the usage of Digital signature. • Plan and implement the security of online services by using PKI	Already started from January 2014	January 2016	MYICT NCSA RURA MoD RDB RNP	1,500,000,000

Government Information Security Management System (G-ISMS) or Government Security Architecture (GSA)	• Review and enhance the developed Government Security Architecture that provides an information Security Management Framework • Plan and raise awareness about GSA • Implement GSA/G-ISMS in the Public and Private Sector.	April 2015	February 2016	MYICT RDB	1,200,000,000
Government Security Certification Program (G-SCP)	• Development of GSC program operational manual and guidance • Training of GSC auditors (technical experts) • Assignment of GSC program operation agencies (policy agency, certification agency)	January 2016	January 2018	MYICT RDB	75,000,000
Cyber Security Capacity Development	• Develop a cyber-security capacity building strategy and Retention Policy • Collaborate with the MINEDUC to include cyber security curriculum for undergraduate/graduate programs • Develop Security Certification Programs for Security Professionals - This 5 year strategy targets to train the following categories in cyber security: a. All Government ICT Engineers and professionals b. Train 400 advanced skills experts in core cyber security. c. Cyber awareness for general ICT users. • Establish a Cyber Security center of excellence in Rwanda	Already started in July 2014	January 2020	MYICT MINEDUC RDB WDA RNP	300,000,000

Cyber Security Awareness	• Develop a cyber-security awareness strategy • Develop annual cyber security awareness programs in public and private sectors and for Internet Home users • Develop Cyber-Security Awareness Materials and dissemination channels	Already started July 2014 ~	January 2020	MYICT RNP RDB	50,000,000
Building Cyber Security Industry	• Cooperate with academia and industry to launch short and the long-term cyber security R&D program • Develop a cyber-security R&D center • Establish a public private partnership to develop cyber security services • Establish a public private partnership to establish cyber security professional training centers	Aready started in July 2014 ~	January	MYICT MINEDUC	2,000,000,000
International Cooperation	• Identify and create membership with Regional and International CERTs (e.g. FIRST, ITU-IMPACT and AfricaCERT) • International cooperation in establishment of cyber law and response to cyber crime • International information sharing and expert exchange • Initiate Cooperative international research and development	January 2016	January 2017	MYICT National CSIRT	100,000,000
					16,855,000,000