

Brief about National Computer Security & Incident Response Center (Rw-CSIRT)

Charles MUGISHA / Rw-CSIRT Manager

July 2016

National Cyber Security Policy

Computer Security and Incident Response Team (Rw-CSIRT)

National Public Key Infrastructure (PKI)

National Cyber Crime Investigation and Digital Forensics Center

Establishment of
Information Infrastructure Security
Systems

Cyber Security
Capacity Building & Awareness

Vision

Ensure Rwandan Cyber Space is Secure and Resilient

Mission

To establish secure and sound cyberspace through early **Detection**, prompt **Response**, and **Prevention** of cyber security incidents

Goals and Objectives

Capability

Response

Cooperation

Monitoring/
Management

Awareness

Capability

To build capability for Detecting, Analyzing and Preventing cyber attacks

- Cultivate cyber security professional personnel to respond to cyber attacks in emerging threats.
- Develop and disseminate technology that could effectively respond and prevent cyber incident

Monitoring/ Management

To assure the security of the computer and network environment in the cyberspace

- Monitor 24/7 To assure the safety and availability of ICT services, Infrastructures, and Networks.
- Security Assessment of ICT services, infrastructure, Networks and manage vulnerabilities.

Response

To establish and operate National cyber security incident response system

- Promptly respond to cyber incidents occurring in both public and private sector.
- Establish incident response system to promptly recover from and handle incident.

Awareness

To raise cyber security awareness to the level comparable to the developed nations

- Establish and operate a platform to timely share and disseminate information about cyber security threats
- Promote awareness about cyber security threats in public and private sector and general public

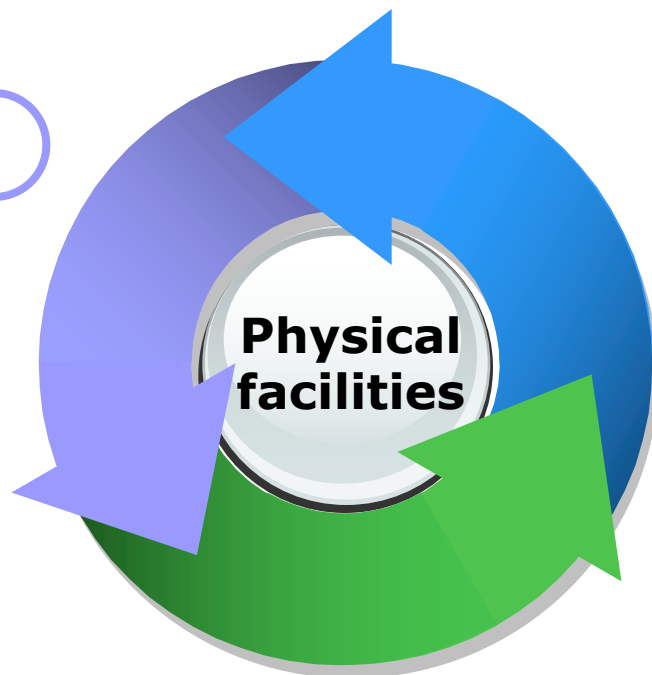
Cooperation

To cooperate with abroad National CSIRTs, and lead the CSIRTs in the Africa

- Establish and operate cooperation and sharing channel between public and private sectors.
- Implement cooperative system with abroad CSIRTs and share information with one another.

Process

- Policies
- Procedures
- Guidelines



Technology

- Security Prevention Systems (e.g. F/W, IPS, WAF, etc....)
- Security Monitoring Solutions (i.e. SIEM Solutions, IDS, etc....)
- Forensics/Analysis Tools

People

- Security Analysts
- Incident Handlers
- Networks Security Engineers
- Systems Security Engineers

Defining Staff Operational Activities



Rw-CSIRT Incident Response System



Security Events Collection Path

Monitoring, Analysis & Response

Prevention Activities

Ministries & Agencies



ISPs





Data Centers





International Partners





Router 


Firewall 

IPS/IDS 

Servers 

Mails 

Tel 

TV 

Internet Traffic
Malicious Content
Vulnerabilities
Incident Reports
Info/News

Rw-CSIRT 24/7



Awareness:

- Security Awareness and Training
- Security Advisory/Alerts & Dissemination

Protection Services:

- Network Protection
- Web App & Systems Protection

Security Consulting:

- Vulnerability Assessment & Patch support
- Penetration Testing
- Policy Development

Forensics:

- Computer Forensics
- Malware Analysis

Q & A?

THANK YOU