REPUBLIC OF RWANDA

MINISTRY OF INTERIOR

MININTER ICT POLICY

August 2024

FOREWORD

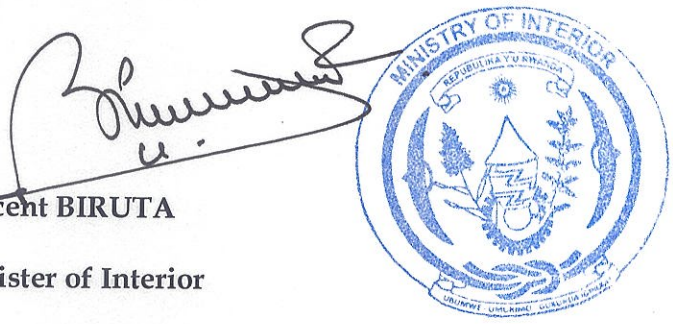
Information and Communication Technology (ICT) is the central engine driving Rwanda's economic transformation and development. It is in this regard that the Ministry of Interior (MININTER) has developed an Internal ICT Policy to facilitate the achievement of its mission.

The MININTER ICT Policy sets guidelines and establishes a framework to be observed and maintained by users in order to create a conducive ICT environment.

The objective of this policy is to ensure MININTER staff use efficiently, effectively and responsibly ICT resources in a secure environment.

All users are responsible for familiarizing themselves with this policy and related procedures.

This policy is in line with laws, regulations and ICT implementation guidelines for the Government of Rwanda.



Vincent BIRUTA

Minister of Interior

LIST OF ACRONYMS

CDO	: Chief Digital Officer
CCTV	: Closed Circuit Television
DAF	: Director of Administration and Finance
GoR	: Government of Rwanda
ICT	: Information and Communication Technology
ID	: Identification
IP	: Internet Protocol
MIFOTRA	: Ministry of Public Service and Labour
MININTER	: Ministry of Interior
NCSA	: National Cyber Security Authority
NDC	: National Data Center
PS	: Permanent Secretary
RISA	: Rwanda Information Society Authority
TV	: Television
VLAN	: Virtual Local Area Network
WIFI	: Wireless Fidelity

TABLE OF CONTENT

1. INTRODUCTION

MININTER is mandated to ensure internal security, peace and stability, and effective correctional services.

ICT infrastructure plays an important role in supporting MININTER to fulfill its mandate as it facilitates the automation of the flow of its information.

The intent of this MININTER ICT Policy is to establish procedures to be followed by MININTER staff in order to ensure the responsible use of the ICT resources in an ethical, legal and secured environment.

This internal ICT policy is in line with national laws and regulations and ICT implementation guidelines for the Government of Rwanda as established by RISA.

2. OBJECTIVES

a. Ensure that staff are fully aware of their responsibilities and obligations regarding the use of ICT;
b. Promote digital solutions;
c. Ensure protection of data and ICT infrastructure;
d. Align ICT with MININTER needs and mission;
e. Ensure effective utilization of ICT resources.

3. SCOPE OF THE POLICY

a. Applies to all units, directorates and departments of MININTER;
b. Covers all MININTER's premises and owned information in all forms;
c. Applies to all end users including permanent, contractors and temporary employees, internees, visitors, consultants, among others;
d. Encompasses all ICT resources within MININTER.

4. ICT COMMITTEE

The ICT Committee is established in accordance with ICT implementation guidelines for the Government of Rwanda. It defines the Ministry's ICT Strategy and ensure all ICT projects in MININTER are well coordinated and aligned to the mandate and overall strategic objectives.

MININTER ICT committee is composed of the CDO, the DAF, the Planning specialist, the ICT Specialist, and the Internal security specialist. The chairperson is the CDO while the secretary is the Planning Specialist. It meets quarterly and reports to the Chief Budget Manager.

5. CAPACITY BUILDING

To ensure coherence, relevance and requisite multiplicity of skills are maintained within the Ministry, a comprehensive ICT training plan will be adopted by MININTER.

5.1. ICT staff training guidelines

- ICT staff perform team and individual self skills assessment, skills development in accordance with respective job profile and duties;
- All ICT training schedules should be done and consolidated at the Ministry level on yearly basis;
- RISA will establish on yearly basis a framework for all ICT training schedules locally, online or abroad.

5.2. ICT users training guidelines

- MININTER staff need to be trained on regular basis, especially when a new technology or new application is introduced;
- MININTER staff training is conducted based on their needs.

6. ICT RESOURCES MANAGEMENT

This policy deals with the process of how the Ministry's ICT resources are procured, received, recorded, stored, distributed, used, maintained, ensured and disposed off. It also indicates levels of classification of ICT resources.

6.1. ICT resources classification

Classification of ICT equipment is done in line with relevant laws, regulations and policies with intent to define their accessibility measures, control and usage.

Classification of ICT resources depends on sensitivity of data and devices, confidentiality, value to the Ministry and levels of responsibility. Each level is associated with access control, security measures and handling procedures.

ICT resources enabling remote access to the Ministry network are subject to stringent security measures.

Categories of ICT resources classification:

- Critical equipment composed of high priority device s crucial for the Ministry operations (Servers, Network infrastructure, Lifts and CCTV system);
- Sensitive equipment composed of devices containing sensitive data or critical to specific functions (Workstations and Databases);
- General equipment composed of standard devices with no critical or sensitive data (General purpose computers, printers and scanners);

- Obsolete or ready for disposal equipment composed of devices subject to disposal procedures.

6.2. Acquisition of ICT Resources

ICT resources are acquired through procurement, donation and grants.

ICT resources acquired through donation are subject to Digitalization office check for suitability and fit-for-purpose.

Acquisition procedures:

- ICT asset acquisition through procurement has to comply with ICT annual procurement plan;
- Upon delivery of the approved ICT resources, notification must be done to the Digitalization office to facilitate installation and addition to the ICT asset register;
- Before acquisition of a new technology, needs assessment is conducted to ensure that the proposed ICT solutions are compatible with the ICT architecture;
- On requisition of a new or modified computing facility, a formal acceptance of the facility is approved by the ICT Committee.

6.3. ICT asset retention

To prevent the deterioration in the productivity of ICT assets, coupled with unacceptable high maintenance costs, a maximum lifespan is allocated to the different categories of these assets:

Description of Asset	Expected Lifespan
Desktop PC's, Laptops, Video/Audio equipment, Monitors, Tablets, Servers.	3 years
Printers, Scanners, Photocopying machine, projectors and TV screens	4 years
Storage devices (external hard disk, flash disk)	2 years
Network switch, routers, Wireless Access Point, WIFI antenna, modems among others.	4 years

An ICT asset to be reused, disposed of, or returned must be erased of any data, information and software.

7. NETWORK INFRASTRUCTURE

The MININTER Network Infrastructure is composed of hardware and software resources that enable connectivity, communication, operations and management of the infrastructure.

7.1. Network use

To establish a robust network Infrastructure, the following practices will be followed:

- The network shall be only accessed by legitimate users with complete and accurate credentials;
- The network utilizes intrusion detection and prevention resources with advanced filtering capabilities to control inbound and outbound traffic, to identify and block malicious activity, and potential security breaches;
- The network uses secure wireless access points with strong encryption and guest network options for limited access;
- The network is segmented into different VLAN to ensure the security of accessible data;
- The core network computer equipment shall be housed in a controlled and secure environment;
- A regular monitoring of network performance, traffic patterns, and security events to identify potential issues and threats before they impact operations shall be done.

7.2. Servers

- The servers shall be registered to ensure that any additions or changes to the network servers have no adverse impact on the network or attached resources;
- The web server, mail server, file server, storage and other relevant computer systems shall be hosted in the National Data Center;
- The servers have to be installed according to clearly defined and documented settings;
- The server room has to be always protected with door access control and accessed only by persons or staff authorized by the CDO or a delegated staff.

8. APPLICATIONS AND THEIR PLATFORM MANAGEMENT

This section covers the applications development and upgrade, email and other platforms usage.

8.1. Applications development, upgrade and customization

- A full detailed analysis shall be conducted by ICT Committee, before developing, upgrading or customizing any application to avoid duplication or develop useless applications;
- Applications development must follow a defined software development lifecycle (SDLC);
- A new application design shall be considered for security, reusability, scalability, interoperability, user satisfaction, productivity, compatibility and cost-effectiveness;
- Any application must be fully documented by providing user procedures, operation and training manuals;
- Applications must be maintained and updated on a regular basis.

8.2. Email usage

- All staff must use official email accounts for official communication and work-related activities in compliance with GoR's e-mail policy;
- MININTER email accounts must have a domain with a suffix of gov.rw e.g. @mininter.gov.rw (cdo@mininter.gov.rw).
- An official email account shall not be linked to a personal email account;
- Confidential information will be secured before sending through e-mail by way of encryption;
- When a staff is no longer the employee of MININTER, his/her official email is revoked after handover;

8.3. Social media and website

- Official social media platforms are managed by the office in charge of communication in collaboration with the Digitalization Office;
- The content for official social media platforms and the website shall be prepared by the office in charge of communication and endorsed by relevant authorities;
- MININTER website shall be designed according to official template for government institutions;
- Web content must be timely updated;
- Social media platforms shall be accessed through MININTER official website.

9. DATA MANAGEMENT AND CYBER SECURITY

This section outlines the data management framework that covers accountability for data, storage, security, maintenance, and dissemination.

9.1. Data management

- Data and information shall be treated with due consciousness;
- Data shall be accessible both onsite and offsite;
- Duplication of data shall be avoided;
- Appropriate backup and disaster recovery measures for all data shall be implemented;
- Backup tools shall be clearly labeled and properly maintained;
- Backups of sensitive data shall be encrypted and monitored regularly to prevent loss.

9.2. Logical security

- All connections to the internet or other public networks shall be protected by firewall configured to filter traffic and prevent unauthorized access to internal resources;
- Data encryption facilities shall be utilized in accordance with ICT implementation guidelines of Government of Rwanda to prevent inappropriate access to sensitive information;
- The user authentication system shall be applied to prevent unauthorized access;
- Regular security awareness programs shall be conducted for end-users to secure data from any attacks;
- Access rights shall be reviewed and confirmed periodically to ensure data security.

9.3. Physical security

- Critical ICT facilities and services shall be restricted to authorized staff by using physical barriers, passwords, locks or access control devices depending on assigned roles and privileges;
- Third parties access to critical ICT facilities and services will be only done under authorization and supervision by digitalization office;
- Fire prevention and detection systems shall be installed near critical ICT facilities and quarterly tested;
- Cooling and humidity control systems shall be installed and kept at optimum levels;
- Disaster control systems shall be deployed in critical ICT facilities.

9.4. Password usage

- All users will be made aware of how to select strong passwords.
- A strong password must be a combination of lowercase, uppercase, numbers and special characters such as! @#${}:">?<; and at least 8 characters in length;

- System-level and user-level passwords must be changed at least every three months;
- Passwords must not be written down on paper, sent through email, included in a non-encrypted stored document, revealed over the phone, revealed or hinted on the Internet, be "remember password" in the application program, be used on unsecured login websites (without https);
- Passwords must not contain common acronyms, have reverse spelling, be easy to guess by using part of your login name and be part of numbers that is easily remembered such as birthdays, phone numbers among others;
- A computer must be set to lock automatically when unattended.

9.5. Environmental Control

- Hazardous or flammable materials must not be stored in the computer facility rooms or nearby critical equipment;
- No unsafe electrical wiring or cluttered areas shall be allowed within the computer facility rooms;
- Air conditioning and humidity controls shall be installed and kept at optimum levels;
- Power protection controls shall be installed to prevent power outages or surges e.g. uninterrupted power supply systems, lighting conductors and backup generators.

9.6. Business continuity and disaster recovery

- The backups shall be encrypted with passwords and restoring from backup shall be tested and documented;
- Disaster recovery training sessions will be conducted to ensure preparedness for a disaster;
- Backup and disaster recovery will follow the directives of National Data Center;
- Daily health checks shall be conducted on critical ICT resources including disk capacity, network bandwidth, buffer sizes, database size, error logs and consumables.

9.7. Cybersecurity

To prevent any cyber-attack, the following measures must be implemented:

- Conduct regular cybersecurity awareness programs;
- Conduct regular vulnerability assessments and penetration testing to identify potential cybersecurity threats and vulnerabilities;
- Access to network resources must be granted or denied based on job functions and related duties;
- Implement system logging;
- Implement network segmentation by classifying network into specific groups and restrict related access through VLANs.

- All security incidences shall be reported immediately to mitigate or to respond as quick as possible to a cyber-incident;
- Discourage connecting suspicious devices on ICT facilities.

10. OBLIGATIONS

This section deals with the obligations on ICT resources for both the MININTER staff and the Digitalization team.

10.1. MININTER staff obligations

a. Professionalism and Compliance

In using MININTER ICT resources, MININTER staff will be required to:

- Ensure compliance with the policy and established procedures;
- Report any ICT-related concerns to the Digitalization Office;
- Report broken IT equipment to the PS and undergo assessment by the Digitalization Office;
- Report stolen computer to the direct supervisor and the PS for further action;
- Report any misuse of ICT equipment or potential threats to the Digitalization Office;
- Report suspected security vulnerabilities or problems with the email system to the Digitalization Office;
- Report any incident or cyber-attack on ICT systems or network to the Digitalization Office.

b. Data Protection and Security

- Ensure privacy and protection of data on their computing devices;
- Acknowledge and take necessary precautions to protect equipment while away from MININTER premises;
- Avoid downloading or distributing malicious software or engaging in illegal or unethical activities using MININTER Internet and computers;
- Avoid opening mail from unknown sources and suspicious attachments or links;
- Use officially authorized antivirus/antimalware on computers;

c. Equipment Usage

- Use ICT equipment for work-related activities;
- Take care of efficient management of printing resources and remove sensitive documents from printers promptly;

d. Internet and Social Media Usage

- Provide only guest network access to visitors;

- Avoid posting inappropriate material on social media that could harm MININTER or its stakeholders.

e. **Software Usage**

Avoid loading shareware, freeware, or open-source software into MININTER ICT assets without permission.

10.2. Digitalization office's obligations

a. **Asset management and distribution**

The digitalization office is required to:

- Distribute ICT assets according to logistics guidelines;
- Authorize and manage the transfer process of ICT equipment;
- Assure proper registration and storage of ICT equipment;
- Regularly report the status of ICT resources.

b. **Security measures**

- Maintain the integrity and security of networked systems;
- Protect all computing devices with licensed antivirus software;
- Ensure that all management interfaces of printers are protected by a password;
- Follow up implementation of passwords policy;
- Establish role-based access controls and implement system logging.

c. **Standardization and maintenance**

- Standardize computer software and hardware for users based on job function, and division;
- Ensure that all machines run on the latest updates/patches' software;
- Take daily, weekly, monthly, and annual backups;
- Plan for ICT hardware maintenance to ensure smooth operations;
- Be equipped with the IT toolbox for relevant computer hardware maintenance.

d. **Network Management**

- Maintain up-to-date network diagrams;
- Provide the wireless and cabling infrastructure supporting voice, data and video services;
- Monitor backbone network traffic to detect unauthorized activities or intrusion attempts;
- Implement the security of the network infrastructure by minimizing exposure to external networks.

e. **Communication and Coordination**

- Communicate planned or unplanned downtime and uptime to employees;
- Coordinate investigations into suspected computer or network security compromises;
- Communicate before scheduled maintenance resulting in service downtime;
- Provide user support on ICT hardware;
- Monitor the website;
- Collaborate with National Data Center in management of hosted MININTER critical systems.

f. **Cybersecurity Measures**

- Regularly perform a security audit of any network device;
- Publish security alerts, vulnerability notices and patches;
- Plan and conduct regular internal cybersecurity awareness sessions for end-users;
- Plan and perform IT infrastructure vulnerability assessment and penetration testing;
- Be prepared to mitigate or respond quickly to a cyber-incident;
- Establish a proper disaster recovery plan to ensure business continuity during emergency.

11. IMPLEMENTATION AND MONITORING

The implementation of internal ICT policy shall be monitored and evaluated by the ICT committee. Evaluation of outcomes of the internal ICT policy shall provide information to which component of the policy is being implemented and the progress made towards achieving policy objectives.

12. AMENDMENT OF ICT POLICY

MININTER ICT policy shall be amended when necessary. The overall policy review shall be undertaken after every 2 years or earlier as need arises and any changes shall be approved by the Management of the Ministry of Interior.

13. BREACH OF THE ICT POLICY

Employees are expected to report any apparent breach of MININTER ICT policy to relevant administrative levels. Failure to comply with this policy may amount to misconduct. Breach of this policy shall be investigated and if confirmed with due proof, it may result into sanctions governed by laws and regulations in place.

Done at Kigali, on 29 August 2024