REPUBLIC OF RWANDA

SOUTHERN PROVINCE
NYAMAGABE DISTRICT
P.O.Box: 36 Gikongoro
Website: www.nyamagabe.gov.rw

E-mail: info@nyamagabe.gov.rw

NYAMAGABE DISTRICT INTERNAL ICT POLICY

This document was prepared by Network and System Administrator to facilitate IT usage in Nyamagabe District

Valid Period: 2022-2025

Prepared by:

NSANZIMANA Eric Thomas
Network and System Administrator

FOREWORD

Information and Communication Technology is a fundamental engine that is driving Rwanda's economy into revolution and development; it is in this context that Nyamagabe District has developed the ICT Policy that will play a key role in guiding the entire staff community and the external users as far as the use of ICT is concerned within the District.

The ICT policy tends to set guiding principle and establish a framework described for projected users to perceive and continue in order to generate conductive ICT environment.

The main objectives of this ICT policy is to encourage Nyamagabe District staff to use correctly the ICT resources available in ethical way, legal and security environment of electronic computing and communication through allowing and supporting them to carry out their daily duties efficiently.

NGARAMBE Alfred
Executive Secretary of Nyamagabe District

Table of contents

AKARERE KA NYAMAGABE

ABREVIATION

1. **CBM: Chief Budget Manager**
2. **DM: Division Manager**
3. **ICT: Information Communication and Technology**
4. **IT: Information Technology**
5. **NSA: Network and System Administrator**
6. **RISA: Rwanda Information Society Authority**
7. **TV: Television**
8. **UPS: Uninterruptible Power Supplier**
9. **VLAN: Virtual Local Area Network**
10. **WIFI: Wireless Fidelity**
11. **NCSA: National Cyber Security Authority**

I.INTRODUCTION

The information and communication Technology (ICT) infrastructure of Nyamagabe district play an important role in assisting Nyamagabe district's staff in rewarding the institution's obligation which in momentary to accomplish the paramount value for currency for the Government of Rwanda.

The main purpose of this ICT policy document; is to establish the guidelines for Nyamagabe district 's staff in order to inspire the responsible use of the ICT resources and establish the proper, lawful and security of electronic computing and communication in Nyamagabe District.

Nyamagabe district's ICT resources are essential to the delivery expected from the District's Staff. The users access the ICT resources in order to enable them to carry out smoothly their duties as well as facilitating the achievement of Nyamagabe district's objectives.

The document establishes framework and describes the standards that users are expected to observes in order to create and maintain a conductive ICT environment.

I.1. Objectives.

The ICT Policy aims to establish usage guidelines for Nyamagabe District's Acquisition, installation and management of all ICT and for employees using Nyamagabe district's computing facilities; including computer hardware, printers, scanners, software applications, e-mail, IP phone, internet and intranet access.

I.1.1 The specific objectives of ICT policy are:

- To Guarantee dependable access to all employees to ICT resources.
- To Safeguard effective use of ICT resources.
- To Train employees about dos and don'ts use of ICT resources.
- Avoid any practice that could destabilize or threaten the reputation of Nyamagabe district, the security of computer network, Nyamagabe District's ICT infrastructure and equipment, data which may expose Nyamagabe district to risk of litigation due to employee misbehavior.
- Monitor Nyamagabe District network and prevent unauthorized access to Nyamagabe district's systems.

- Prevent misappropriation to computer or data.

I.2. Scope

These strategies spread over to all Nyamagabe District 's employees and other workers based in Nyamagabe district, who use the institution's computing facilities and cover all information and communication Technology properties including both hardware and software that is owned or leased by Nyamagabe District. Nevertheless, Nyamagabe district's Network and System Administrator is not responsible for privately owned equipment and their usage should have limited on Nyamagabe district's network protection measure. Users of ICT in Nyamagabe district should mindful that the data created by Nyamagabe district or with Nyamagabe district owned software, remains the property of Nyamagabe district.

The use of Nyamagabe district's ICT resources involves any user to fulfill with monitoring and expose establishment of these guidelines.

II. NETWORK AND COMMUNICATION INFRASTRUCTURE

Nyamagabe District provides network services to large number and variety of users, including staff and external constituencies. Network and communication infrastructure of Nyamagabe district is composed of hardware (wireless access points, Cables, Racks, UPS, Routers, Firewall, Switches, etc…) and software resources of an entire network that enable network connectivity, communication, operation and management of Nyamagabe district network.

II.1. Network design

Nyamagabe district's network shall be segmented into different VLAN to ensure the security of accessible data. ICT steering committee will maintain up to date network diagrams (Both logical and physical) that define the network topology. IP address, Core network equipment etc. for all networks that they are responsible.

II.2. Network implementation

Network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate credentials. Network must be able to with stand or recover from threats to its availability, integrity and confidentiality. Core network computer equipment will be housed in controlled and secure environment.

II.3 Network Management

- Network and System Administrator (NSA) is responsible to communicate planned or unplanned downtime and the uptime to employees through appropriate means of communication with 30 minutes of downtimes.
- NSA is responsible to perform a security audit of any Nyamagabe district network device at any time.
- NSA is the primary administrative contact for all Nyamagabe district network security related activities.
- NSA will prepare recommendation and guidelines for network and system administration.
- In collaboration with NCSA, NSA will publish security alerts, vulnerability notices and patches and other relevant information in an effort to prevent security breaches.
- NSA will coordinate investigation into any suspected computer or network security compromises, incidents and any other problems.
- NSA will monitor backbone network traffic in real-time to detect unauthorized activity or intrusion attempts.
- NSA has right to remove any network segment from the Nyamagabe district network until problems affecting the network are identified and solved.
- All network users are responsible for understanding this policy and its applications
- NSA is responsible for ensuring that a log faults on the core IT network is maintained and reviewed.
- NSA will review network security best practices on an annual basics and recommend changes to this policy.

II.4. Internet usage

- All users shall use or access the internet for non-business purposes and restrict personal use to minimum limited to educational, communication, knowledge and news sites.
- All users shall not use Internet facilities to download or distribute malicious software or tools or to deliberately propagate any virus.
- All users shall not violate any copyright or license agreement by downloading or distributing protected material.

- All users shall not conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting Nyamagabe district.
- All visitors shall have their own separate internet access.

III. HARDWARE AND END-USER EQUIPMENT

III. 1 Introduction

The Hardware constitutes the physical computing equipment and resources used by consumers in their daily activities.

Nyamagabe District's ICT hardware devices include laptop computers, desktops, servers, printers, scanners, cameras, projectors, TV sets, routers, access points, switches, fingerprint machines, individual PCs, notebooks, PDAs, and other such devices (to be referred to as "workstations"), among other sophisticated IT equipment that are acquired through purchase or donation.

III.2 ICT Hardware Distribution

- All ICT hardware acquired by Nyamagabe District end-users should comply with ICT hardware annual procurement plan.
- Distribution of ICT hardware must only be handled by Administration unit and comply with logistics guidelines.
- ICT hardware must not be connected, installed or operated within Nyamagabe district without authorization of the Administration unit.
- No ICT hardware will be given to any end-user without formal authorization of logistics office.

III.3. ICT Hardware Usage

- All ICT hardware must serve the purpose that it was purchased for; unless authorized by logistics office based on request from user department approved by his/her supervisor.
- ICT hardware usage must be monitored and reported to administration unit and Logistics office for appropriate measures.
- Any liquid and food products should be avoided in the proximity of hardware devices.
- NSA shall standardize computer software and hardware for users based on but not limited to job function, division and the least privilege principle. This will help to avoid unnecessary costs.

AKARERE KA NYAMAGABE

- In case a user requires a specialized hardware than the current standard, the user shall request for this in writing to the CBM of Nyamagabe district. Nyamagabe district shall at its discretion evaluate the merits of each hardware request.
- All users shall be responsible for the assigned IT equipment even if the IT asset is out of its life span.
- The broken IT equipment shall be reported to the ICT office, the assessment shall be made for identifying the ways the equipment has been broken or damaged, and the appropriate measure shall be taken.

III.4 ICT Asset retention

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

Description of Asset	**Expected Lifespan**
Storage devices (external hard disk, flash disk)	2 years
ICT toolkit	3 Years
Network switch, routers, Wireless Access point and WIFI antenna	3 years
Desktop PC's, Laptops, Audio equipment, monitors, TV screens, tablets and Servers	3 years
Printers, Scanners, Photocopying Machine and Projectors	3 Years

III.5 Donations and grants

All ICT hardware donations and grants to Nyamagabe District from any source are subject to be checked by the NSA for its suitability, fit-for-purpose and ensure the equity in distribution.

III.6 ICT Hardware Security and Disaster Management

- To prevent theft or loss of unattended ICT hardware, all portable devices shall be kept, where possible, out of sight and preferably in a locked environment.
- The line managers and ICT office shall be formally notified of any damage or theft of ICT hardware peripherals.
- The administration unit via line management shall be requested to make changes regarding relocation of ICT hardware and peripherals.
- All ICT Hardware and peripherals belonging to Nyamagabe district shall bear appropriate insurance (In the insurance of all Nyamagabe district's asset).
- ICT hardware must only be disposed in line with national disposal policy and procedures in place.

IV. Software Application and Data

Software includes all Nyamagabe district's databases, operating systems, antivirus, Microsoft office applications and any other software residing on Nyamagabe district's equipment.

This section of the policy will cover the acquisition of software and licensing, application development and upgrade, email and other platform usage.

IV.1. Applications Development, upgrade and Customization

- For all applications to be developed, upgraded and customized, NSA in collaboration with RISA, she/he must provide a full detailed analysis of what is required to avoid getting useless applications.
- All applications development, upgrades and customization requests shall be authorized by CBM of Nyamagabe district and approved by RISA.
- Each application designed, upgraded or customized for Nyamagabe district must be full documented: the documentation has to always include a well done user manual and the administration training manual.
- Each application designed, upgraded or customized for Nyamagabe district must be handed over with application source code depending on the service level agreement. All applications developed, upgraded or customized shall be fully owned by Nyamagabe district.

IV.2. Software Security

By software security the document refers to ability of software to continue performing even under malicious attacks. NSA is responsible of ensuring that software, especially tailor developed application, are designed in manner to withstand attacks proactively or at least recover from attacks.

IV.3. Viruses and Other Harmful Application

- NSA must ensure that an effective and licensed anti-virus system is installed and functional on all computing equipment.
- Nyamagabe district's employees must work to prevent the receipt and transmission by any means (email or physical device) of malicious software, especially viruses. This implies the minimum usage of removable disks, especially when they have been in different locations whose security is not assured. It also means that external disks or downloaded or distribute files must be scanned for viruses before being connected or loaded to Nyamagabe district network.
- It is prohibiting to load, download or distribute any information or materials that may corrupt or affect the security of Nyamagabe district's computer network.

IV.4. Data Management

- NSA has to define the logical process of data filing framework from individual end-user to institutional level.
- All data and information should be treated with due consciousness.
- All staff must ensure the confidentiality, integrity and privacy of the data maintained and backups.
- Appropriate backups and disaster recovery measures shall be administered and deployed for all Nyamagabe district data.
- Backups tools (Storage media, shared cloud platforms, etc...) must be clearly labeled and properly maintained
- Any requirement to access restricted data must be approved by the CBM or DM of Nyamagabe district on needed data.
- It is highly discouraged to connect suspicious devices on Nyamagabe district ICT facilities.

V. SYSTEM ADMINISTRATION

V.1 Password protection

- All users must use strong password (combination of lowercase, uppercase. numbers and special characters) at least 10 characters in length.
- All users must change passwords regularly in 90 days and automatically whenever there is any indication of possible system or password compromise.
- Users will not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical user accounts shall be maintained securely.
- Users shall not share their passwords unless authorized by NSA.

V.2.E-mail account

Employees 'emails allowed for work or personal use. But users are required to make sure circulated materials to or from the internet are not harmful (don't contain viruses), obscene or illegal.

- All Nyamagabe district staff must have Nyamagabe district's official email (**@nyamagabe.gov.rw**).
- All staff are obligated to use Nyamagabe district staff's official email for official communications and when doing Nyamagabe district related activities.
- Personal emails such of these domains (Google, Yahoo, Hotmail, Microsoft;…) are not allowed for official communication and when involving Nyamagabe District related activities.
- After cessation of a staff, his/her official email must be blocked after handover and deleted after 3 month of cessation.
- Unsolicited mail messages, including "junk mail" or other advertising material should not be sent to individual or user groups.

V.4. System Access

- NSA should ensure systems availability and whenever there is an interruption beyond control, users should be immediately notified on what is the issue, what is being done to correct it and when they can expect services to be restored.

- Work related data must be backed up for business continuity. Nyamagabe district through NSA has to assure that in case of an incident, users 'data can be recovered. Nyamagabe district is not responsible for personal data, and this must not be stored in its servers.
- NSA is responsible to put in place a backup system and notify users of its functionality and provide support whenever needed.

VI. CYBER SECURITY

Taking action to ensure computer security helps protect everyone from data and identity theft, viruses, hackers and other treats. All users are expected to follow and implement these security guidelines.

VI.1. Access control

- Identification, authentication and authorization are control to access to Nyamagabe district's computing facilities.
- Each user is responsible for ensuring that access to his/ her computing device is protected.
- All users are required to abide to this rule and no one is allowed by someone's ID and password.
- Password must be changed regularly. But in case there is a doubt that it has been compromised, it should be changed immediately. This also applies for login ID. IT resources should be designed to default no access in the event of malfunction. this is a denial of privileges to end users until all come to normal.

VI.2. Network security

Nyamagabe district network must be designed and implemented in a manner to minimize any intrusion and unauthorized access. Nyamagabe district Local Area Network should protected by firewall and all computers connected to Nyamagabe district network should have anti-malware software (up-to dated) including servers. Nyamagabe district local area network and wireless should use IPs and Password to avoid unauthorized use of networks and avoid attacks from outside.

Remote access to Nyamagabe District networks must be strictly limited to high profile users. A remote user's computer must be at least as secure as its onsite counterpart. All devices connected to the network, including core routing and switching, wireless and firewalls, need periodic assessment in order to protect the integrity of Nyamagabe district infrastructure. Given the

sensitivity of the office, Nyamagabe district has to conduct regular security audit on its network to prevent from unauthorized access and allow further measures to be taken to strengthen security.

NSA has the right to remove from the network any user who is believed, by his/her activities, to constitutes a security breach in the network until all corrections and measures to fix the situation are made.

VI.3. Physical security

- All equipment must be cared for each employee is responsible for the physical security of his/her computer equipment.
- User must avoid for example spilling liquids on them and protect them, where possible from physical damage.
- The server room should also be protected in physical secure location with controlled access.
- NSA holds responsibility to ensure access to server room and data stored on them are strictly limited to authorized users.

VI.4. Download

- Downloading is allowed for attachment only. In case of free software to be downloaded from the internet, user need to get the approval from ICT department. This is part of security measure.

VI.5. Logical Security

- All connections to the internet or other public networks must be protected by firewall configured to filter traffic and ensure against denial of service attacks and unauthorized access to internal resources.
- Data encryption facilities must be utilized in accordance with ICT Implementation guidelines of Government of Rwanda.
- User authentication system must be applied to prevent unauthorized access to the internal resources.
- NSA must ensure that effective and licensed anti-virus system is installed on computing equipment.

- Regular security awareness programs shall be conducted for end-users and system administrators to secure institution's data and information from any attacks.

VII. ICT HARDWARE AND SOFTWARE ACQUISITION

- For each year, users submit their requirements in terms of equipment and software to be purchased. Depending on the available budget, ICT Steering committee must accept the acquisition and confirm that acquired equipment meet standards and up-to-date technology
- Old and malfunctioning equipment to be replaced must be evaluated before any decision to buy new equipment is done to avoid wasting he country's resources on equipment which are not really needed.
- Software to be purchased, operating system, anti-virus or any other software must be licensed. Network and system Administrator has the mandate to ensure that licenses of software running on computer equipment are still valid.

VII.1. Acquisition of Software and licensing

- The acquisition of software and licensing shall be acquired basing on the Rwandan Procurement Laws and guidelines expect for donor funds that may state otherwise.
- Software to be purchased must be licensed and NSA has the mandate to ensure that licenses of software running on computing devices are still valid.
- Software acquired through any processes must be inspected and approved by the NSA for compatibility during the acquisition process.
- Notification to the NSA must be made upon delivery to facilitate the installation of new supplied software to the Nyamagabe district's computing devices.
- Software on multiple machines may only be installed in accordance with to be applicable license agreements.
- No shareware or freeware and open source software should be loaded onto Nyamagabe district ICT assets without written permission of CBM

VII.2. Acquisition of ICT Hardware

- Acquisition of ICT hardware must be in accordance with the Rwandan Public Procurement law, policies, regulations and procedures.
- NSA must be consulted in all procurement of ICT equipment and software.
- Equipment acquired must be inspected by NSA and approved by the CBM of Nyamagabe district for compatibility during the acquisition process.
- Notification to the Logistics must be made upon delivery to facilitate the addition of the equipment to the ICT asset register.
- Before IT equipment and software are acquired they must be investigated. There must be a valid business requirement with a formal definition of information requirements that agreed between the user and ICT section.

VIII. ENVIRONMENTAL CONTROL

- All users must take reasonable steps to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery.
- Hazardous or flammable materials shall not be stored in the computer facilities rooms or nearby any other critical information processing equipment.
- Eating, drinking or smoking inside the computer facilities rooms is strictly prohibited.
- Dust covers must be used to protect critical information processing equipment
- No unsafe electrical wiring or cluttered areas are allowed within the computer facilities

IX. BACKUP AND DISASTER RECOVERY

- NSA is responsible for taking daily, weekly, monthly and annually backups.
- The backups shall be encrypted with password.
- Restoring from backup exercises shall be tested and documented.
- Disaster recovery training sessions must be conducted to ensure preparedness fora disaster
- Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user.
- It is imperative that end-users save their data to the appropriate media and/or network space outlined in this policy in order that their data is backed up regularly in accordance with Nyamagabe district regulations and business continuity plans.

- This policy does not cover end-user information that is saved on a network or shared drive, as these are backed up when the servers are backed up.

IX.1 Onsite-backup

- A backup copy of any valuable data stored on Nyamagabe district's computers should be kept intact. Every Nyamagabe district staff should always save work related documents in backup folder located on the desktop of his/her computer and he/ she must make and handle to NSA a backup copy of that folder to be store on backup server every month.
- Data on server must be saved and stored in the dedicated data storage area. These dedicated storage areas are responsibility of NSA.

IX.2. Offsite-backup

Data of Nyamagabe district should be stored in national data center through the contract of backup with AOS Ltd payed annually.

X.ICT SUPPORT SERVICES

The ICT support shall cater for all areas under the Nyamagabe district network, computing devices, hardware, software and implementation of ICT initiatives at all Nyamagabe district's premises and their related technical support.

This policy describes how the ICT hardware support services, maintenance and repair shall be provided to the end-users.

X.1. Users' support

- NSA provides tier support to all end-users on ICT hardware for work related processes only.
- NSA must design the way user support shall unlock effective and efficient use of the ICT hardware. Some Issues that can be considered in the design include but not limited to:
- Capacity building to operationalize acquired ICT hardware to all end-users.
- Priority defined in terms of profile of the user requesting support, number of employees affected by the issue, urgency of the fix, etc...
- Feedback from users to help measure user's satisfaction in ICT services.

AKARERE KA NYAMAGABE

X.1. Maintenance

NSA organizes maintenance: How it is done, the timetable and expected output. Small works, like fixing equipment may be undertaken by NSA staff. However, Nyamagabe district must hire an ICT maintenance company to avoid having to go through tender whenever an important problem occurs. This company must provide a detailed plan of the work including description of tasks to be carried and the result to be expected.

X. 2. Repairs

ICT hardware that need to be repaired outside the Nyamagabe District premises must be registered and have a complete file describing the issue and action to be taken, recommendations and formally authorized. Equipment must be delivered to the ICT office during regular business hours. ICT Department will be available from Monday to Friday between 7 am and 5 p.m. to receive equipment, or by special arrangement by calling **3201** or by e-mail (network@nyamagabe.gov.rw)

X.3. Training

ICT being one of the fastest evolving technologies, NSA staff and users need to be trained on regular basis especially when a new technology or new application is introduced. if any user is unfamiliar with any application /device or need to be able to use it effectively, it is advised that the user may inform respective supervisor about arranging the appropriate training in consultation with NSA staff.

In house training must be conducted every year for employees who are not familiar with systems. These training must be based on users 'needs which are most of the time different from one user to another.

NSA staff must also be trained as often as possible to keep them updated on the current technologies. It will be done in collaboration with Rwanda's institution in charge of NSA in its capacity building program and in case of particular area of expertise which is not provided by the above institution, special arrangements may occur.

XI. IMPLEMENTATION AND MONITORS OF THIS INTERNAL ICT POLICY

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

XII. BREACH OF THE NYAMAGABE DISTRICT ICT POLICY

Employees are expected to report any apparent breach of these guidelines to their higher authority. Any equipment damaged, lost or stolen while under the care of Nyamagabe district staff, shall be paid back by the responsible person unless it is proved that the loss could not have been avoided. Failure to comply with this policy may amount to misconduct. Apparent breaches to this policy will be investigated and if confirmed with due proof, it may result to disciplinary action, including dismissal in the case of serious or persistent breaches.