NIRDA

National Industrial
Research and Development
Agency

INTERNAL ICT POLICY

January 2023

FOREWORD

Information and communication technology (ICT) is the central engine that is driving Rwanda's economy into transformation and development. It is in this regard that the National Industrial Research and Development Agency (**NIRDA**) has developed an Internal ICT policy that will play a key role in assisting its employees in meeting its mission.

The internal ICT Policy intends to set guidelines and establish a framework described for expected users to observe and maintain in order to create a conducive ICT environment. All users are responsible for familiarizing themselves with this policy and related policies and procedures, as appropriate to their role within the Institution.

The main aim and objective of this internal ICT Policy are to encourage NIRDA staff to use responsibly ICT resources in an ethical, legal, and secure environment of electronic computing communication by enabling and assisting them to carry out their duties efficiently and effectively.

Dr. Christian SEKOMO BIRAME

Director General

Signature : ----------

LIST OF ACRONYMS

CBM	: Chief Budget Manager
GoR	: Government of Rwanda
ICT	: Information and Communications Technology
ID	: Identification
IP	: Internet Protocol
NIRDA	: National Industrial Research and Development Agency
RISA	: Rwanda Information Society Authority
TV	: Television
VLAN	: Virtual Local Area Network
WIFI	: Wireless Fidelity
DAF	: Director of Administration and Finance

Table of Contents

1. INTRODUCTION

The National Industrial Research and Development Agency (NIRDA), is a government institution that has been mandated with a mission to enable a generation of industrial innovators to become competitive through technology monitoring, acquisition, development, and transfer & applied research.

Mission

Enabling a generation of industrial innovators to become competitive through technology monitoring, acquisition, development and transfer and applied research.

Vision

To be recognized as a Centre of excellence in the provision of technology support services to increase the competitiveness of Rwandan industries.

The main objectives of the National Industrial Research and Development Agency is to Improve the competitiveness of existing industries in order to increase their export potential or their potential to undertake import substitution, and identify new sub-sectors or value chains where investment by the private sector would likely lead to export growth or import substitution.

Information and Communication Technology (ICT) infrastructure of NIRDA plays an important role in supporting NIRDA to fulfill its mandate by automating the flow of information within the Institution.

The intent of this ICT policy is to reduce unnecessary ICT expenditure and ensure proper usage of ICT resources and services.

This internal ICT policy is in line with ICT implementation guidelines for the Government of Rwanda established by the Rwanda Information Society Authority (RISA).

2. OBJECTIVES OF THE INTERNAL ICT POLICY

The purpose of this internal ICT policy is to clearly establish a set of procedures reflecting management's guidance and directions of controls over information and communication technology in order to improve ICT equipment maintenance, reduce unnecessary ICT expenditure and ensure proper usage of ICT resources,

Specifically, this ICT policy aims at:

i. Ensuring that staff is fully aware of their roles, responsibilities, and obligations regarding the use of ICT assets and services.

ii. Ensuring the institution's data privacy and protection on all ICT premises
iii. Defining, describing, and communicating to end users the acceptable usage of computing devices and other peripheral devices.
iv. Ensuring all ICT activities are aligned with NIRDA's needs and objectives.
v. Communicating to all end users NIRDA's requirements regarding the acquisition, distribution, and disposal of ICT hardware.
vi. Improving the effective utilization of ICT resources.
vii. Preventing any usage that could undermine or threaten the reputation of ICT infrastructure which may expose NIRDA to the risk of litigation due to staff and end-user misuse.

3. SCOPE OF THIS INTERNAL ICT POLICY

NIRDA ICT policy is defined in line with ICT Implementation guidelines for the government of Rwanda established by Rwanda Information Society Authority (RISA).

It is applicable to all NIRDA staff including interns, authorized guests, and contractors who use, access, or otherwise employ locally or remotely NIRDA's ICT resources, whether individually controlled, shared stand-alone, or networked.

4. NETWORK AND COMMUNICATION INFRASTRUCTURE

a. Network design

The network of NIRDA shall be designed to include all departments and units within the Institution and in conformity with requirements preset by the line ministry through the digitalization office.

The design of the NIRDA network diagram shall consider the number of users based on the organizational structure, interior design of the building, sitting arrangement, systems, services, and applications according to the institutional business processes.

The design of the NIRDA network diagram shall consider network security in compliance with the measures defined by the Rwanda Information Society Authority (RISA) and shall continuously adapt to comply with the cyber security directives for government institutions.

b. Network Implementation

The network implementation shall include Network and communication infrastructure such as routers, switches, network cabling, network cabinet, WI-FI access point, patch panel, firewalls, Modems, and software resources of an entire network that enable network connectivity, communication, and operations on NIRDA network.

c. Network management

In conjunction with the Internet Service provider (ISP), the monitoring and maintenance of network performance shall include: Redundancy, load balancing, quality of service control & assurance, and ensure that:

- The Network is availed and managed by ICT personnel and can be accessed only by legitimate users.
- The NIRDA ICT personnel under the supervision of the digitalization office (MINICOM) shall segment the network into different virtual local area networks (VLAN) to ensure the security of accessible data.
- The NIRDA ICT personnel shall avail to all visitors of the wireless Local Area Network (WLAN) for ensuring security of data.
- The NIRDA ICT personnel shall maintain up to date network diagrams (both logical and physical) that define the network topology, IP addresses, core network equipment etc. for all networks that they are responsible.
- The core network computer equipment's shall be kept in a defined server room complied with the latest standard as guided by RISA.
- The NIRDA ICT personnel shall be responsible to communicate planned or unplanned network downtime and the uptime to the employees through appropriate communication means within 30 minutes of downtime.
- The NIRDA ICT personnel shall publish security alerts, vulnerability notices and patches, and other relevant information in an effort to prevent security breaches.
- The NIRDA ICT personnel shall remove any network segment from the NIRDA network until problems occurred affecting the network are identified and solved.
- The NIRDA ICT personnel shall be responsible for ensuring that log faults on the core IT network are maintained and reviewed.
- Access rights and Privileges to Contractors / Outsourcers shall be assigned/granted based on the terms under the Contract and Non-disclosure agreement.
- Confidential data should not be stored in a public or open-access folder. If there is a need to share or transmit confidential data, it must be stored in a secured shared folder or password protected or encrypted.

5. HARDWARE & END USER EQUIPMENT

ICT hardware and end-user equipment shall include servers, laptops, desktops, uninterruptible power supply (UPS), tablets, racks, printers, scanners, cameras, projectors, TV sets, routers, WI-FI access points, switches, fingerprint machines, Air Conditioners, among other sophisticated IT equipment that are acquired through purchase.

The following measures and procedures share be applied to servers, computers and communication devices, powers supply and backups, scanners and printers and all remaining end user's equipment:

- All ICT equipment's shall be defined and designed by the NIRDA ICT personnel after circulation of an ICT needs template to all department for consolidation and approval by Chief Budget Manager.
- Hardware purchased through procurement process shall be in accordance with the Rwandan Public Procurement law, policies, regulations and procedures.
- The NIRDA ICT personnel shall be consulted in all procurement of ICT equipment and software.
- All ICT equipment acquired shall be inspected and approved by the NIRDA ICT personnel together with NIRDA receiving committee for compatibility during the acquisition process.
- All ICT hardware donations and grants to NIRDA from any source are subject to the NIRDA ICT personnel and NIRDA valuation committee and check for suitability, fit-for-purpose and ensure equity in distribution.
- All ICT hardware that belongs to NIRDA shall bear a unique identification code and appropriately stored.
- Logistic office shall issue ICT stock request forms to whoever need hardware equipment from stock.
- The request of IT Equipment shall be initiated by user department/NIRDA Staff, approved by direct supervisor, verified by NIRDA ICT personnel, authorized by Director of Administration and Finance (DAF) and distributed by logistics office.
- All ICT hardware shall serve the purpose that it was purchased for, and ICT personnel shall ensure the monitoring of use on quarterly basis.
- All shared ICT hardware assets to be used for special occasions (e.g.: projectors, printers, cameras, etc...) shall be initiated by the user department/NIRDA Staff, approved by the direct supervisor, verified by the NIRDA ICT personnel, authorized by Director of Administration and Finance (DAF) and distributed by logistics office.
- ICT hardware shall not be connected, installed, or operated within NIRDA without the authorization of the ICT Personnel.
- The NIRDA ICT Personnel 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.
- In case a user requires specialized hardware than the current standard, the user shall request for this in writing to the Director of Administration and Finance and shall at its discretion evaluate the merits of each hardware request.
- Computer machines shall be replaced upon submission of a replacement request form duly filled by the user i.e. User Name, Department, Computer description Model, Serial No and Job Position, and the reason for the replacement request. This form must be

signed by the Head of the user's department and forwarded to the NIRDA ICT personnel for verification then submitted to Logistics. The replacement can only be done on a priority case by case basis and where

- The user machine has undergone severe/ critical hardware failure that is beyond repair.
- The user machine is old (at least 2 years) and is problematic.
- The user machine is lost/stolen, in such a case the details surrounding this must be properly documented and such cases must be reported to RIB.

- Where a computer machine is deemed to be serviceable and requires hardware upgrade etc, the end user shall be advised accordingly and the procurement request shall be for procurement of computer part/s.
- Where a user computer is damaged/ faulty due to negligence and/or carelessness on the user; the user shall be surcharged the cost of repairing/replacement of the hardware. This shall form the basis of any further procurement of replacement computers.
- No non portable ICT equipment shall be moved from NIRDA premises and from one office to another unless there is a formal request initiated by user department/NIRDA Staff, approved by direct supervisor, verified by NIRDA ICT personnel, authorized by Director of Administration and Finance (DAF) and distributed by logistics office.
- ICT hardware shall be handed over to the logistic office after verification of equipment status, initiated by user department/NIRDA Staff, approved by the direct supervisor, verified by NIRDA ICT personnel, authorized by the Director of Administration and Finance (DAF,) and received by logistics office when the user is not in need or is no longer employee of NIRDA.
- The transfer, donation, and disposal of all ICT hardware shall be prepared by NIRDA ICT personnel together with the NIRDA valuation committee and approved by CBM.
- The NIRDA ICT personnel shall provide preventative maintenance support i.e. updating of antivirus, installation of patches, and other services on a schedule such users must avail their machines for service maintenance when required and if unavailable must make other arrangements with NIRDA ICT personnel for such maintenance to be done.
- Any issued ICT hardware that is stolen must be reported to RIB within 24 hours of the theft, and a RIB report or declaration shall be then submitted to CBM and the appropriate measures shall be taken as outlined in the Human Resources Management Manual.

- All users shall be responsible for the assigned IT equipment even if the ICT asset is out of its life span. The broken IT equipment shall be reported to DAF, NIRDA ICT personnel and the logistics office shall asses the ways equipment has been broken or damaged and the appropriate measure shall be taken as outlined in the Human Resource Management Manual.
- Depreciated or damaged ICT hardware devices should be collected for disposal after the assessment report of the NIRDA ICT personnel and logistic office approved by DAF, the disposal shall be made in line with national disposal policy and procedures in place.

- NIRDA ICT personnel shall be responsible for any shared ICT asset such as a Printer, photocopying machine, or shared scanner among different users.

- Any damage of ICT asset due to mishandling or negligence of the employee concerned shall be liable for action as per the human resource management guidelines.
- Employees shall be responsible to keep food and drink items away from IT asset under his / her custody.
- It should be ensured that the ICT asset is not kept near the combustible material, water tanks or basins, below air conditioner units and unmanned public area.
- If a PC is temporarily not in use at any time during the day, the screen should be locked and turned off.
- The PC, Laptop, printer, scanner, or reader shall always be shut down at end of the day, or at such other time as may be necessary.
- The Security concerned shall not allow the movement of any ICT asset outside the institution's premises without the signed Gate Pass.
- Employee shall ensure appropriate disposal of waste media such as printed statements, damaged magnetic tapes, faulty hard disks, unused CDs, Pin, cards, etc.... under their custody.
- The NIRDA ICT personnel shall be responsible for disabling all unused data, voice, and UPS points that are located in the public area.
- All data cables shall be concealed or hidden so that it is not accessible easily to anyone.
- 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 NIRDA ICT personnel shall be formally notified of any damage to ICT hardware peripherals.
- All ICT Hardware and peripherals belonging to NIRDA shall bear appropriate insurance (Covered in the insurance of all assets).
- All users shall 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 or while using a computer is strictly prohibited.
- Dust covers shall be used to protect critical information processing equipment.
- Human-friendly fire prevention and detection systems must be installed in the computer facilities rooms and must be regularly tested.
- Air conditioning, ventilation, and humidity controls shall be installed and kept at optimum levels.
- Enough drainage shall be employed in computer facilities rooms to prevent flooding. Hardware.

6. HARDWARE MAINTENANCE

ICT hardware shall be maintained by NIRDA ICT personnel across their full lifecycle from acquisition to disposal. The preventive maintenance shall be made by NIRDA ICT personnel in collaboration with the hired company at least quarterly or when a curative maintenance need arises by the user department.

All the After the warranty period, there should be agreements with equipment suppliers and services providers such that maintenance services shall be provided at least every quarter. Extended service items such as refresh training, preventive visits, small curative maintenance, and trade-in benefits shall be captured in a contract where each type of contract is reviewed and evaluated on its own merit.

7. SOFTWARE APPLICATIONS AND DATA

Software infrastructure of NIRDA shall include operating systems, antivirus, Microsoft Office applications, Portals, and any other software residing on NIRDA's equipment.

a. Software purchase and installation

- NIRDA in its financial and administrative autonomous status shall procure the required IT equipment and accessories through RISA framework contracts with its suppliers, NIRDA may decide to issue purchase orders for the acquisition of needed items.

- The acquisition of software and/or licensing shall be prepared by the NIRDA user department in collaboration with ICT Personnel through the Digitalization office on behalf of public institutions, except for donor-funded that may state otherwise

- Software to be purchased shall be licensed and NIRDA ICT Personnel has the mandate to ensure that licenses of software running on computing devices are still valid.

- Software on multiple machines shall only be installed in accordance with the applicable license agreements under guidance of RISA.
- Software acquired through any processes shall be inspected and approved by NIRDA ICT personnel in collaboration with the digitalization office and RISA for any issue that may rise during the acquisition process and received by NIRDA receiving committee.

- No shareware or freeware and open-source software shall be loaded onto NIRDA ICT assets without written approval from the relevant authority.

b. Data

Any requirement to access restricted data must be approved by the Director General depending on needed data.

Data to be protected are: OS, Application and Databases, Emails and data on personal computers. Users must take note that they share the responsibility of data availability and integrity even if NIRDA owns any work-related data, on any issued NIRDA ICT equipment.

The NIRDA ICT personnel shall insure that all NIRDA's applications accessed by external users are hosted in National Data Center for security purpose.

This team shall communicate to all end users the best way of filing their data in computer.

The NIRDA ICT personnel shall work with employees to create folders according to their produced or received key documents.

All data shall be stored in a partitioned local disk other than local disk C: and for security purposes, a copy should be automatically kept on the backup server on regular basis and the concerned staff reserves the responsibility to keep a different copy of his/her important data on a removable disk and/or on NIRDA cloud services. Frequencies of automatic backup (daily, weekly or monthly) will be determined depending on the sensibility of the data.

Employees shall ensure that the confidentiality, integrity, and privacy of the data are maintained by using different security mechanisms such as passwords, PINs, fingerprints, etc...

The staff in possession of NIRDA data must ensure that the data in question are kept safe and not shared with unauthorized personnel.

c. Password Protection

Password shall not be written down on paper, password shall not be included in a non-encrypted stored document, password shall not be sent through email account that does not have a secure login (https).

Password shall not be revealed over the phone, shall not be revealed or hinted on a form on the internet; password shall not be "remembered" if the "remember password" feature in the application program such as Internet Explorer, Google Chrome, safari and Mozilla Firefox is used.

Password shall not contain common acronyms; password shall not have reverse spelling; password shall not use part of your login name; and password shall not have part of numbers easily remembered such as birthdays, phone numbers, etc...

A password shall have a minimum of 8 characters. The minimum complexity of password shall use a lowercase, uppercase, numbers and special character (!@#$%)?.). Password age should not be more than six (6) months unless otherwise advised by the ICT Personnel.

d. Email Accounts

- Every NIRDA employee (permanent and temporally) consultant and any other person approved by the CBM shall have NIRDA email account and he or she is obliged to use it for official communication and only work-related activities.
- Request to open or close an email account must follow NIRDA process for joining and leaving the institution as per Human Resource Management guidelines.
- The official email account shall not be linked to personal email account.
- Employee shall not send large file attachments (over 20Mb) to many email addresses. Users shall compress attachments to reduce the size to below 20MB or better still consult the NIRDA ICT personnel for support
- After cessation of a staff, DAF shall request the NIRDA ICT personnel to lock his/her official email after handover.
- Unsolicited email messages including junk emails or other advertising materials shall not be sent to individuals or user groups or replied to. It is advisable that such junk emails shall be deleted or reported to the NIRDA ICT personnel.
- The Email facility shall be withdrawn or restricted by the Director General without prior notice in case the Employee does not comply with the e-mail policies.

- When out of office or on vacation, the user should leave an out-of-office message via the web-access that states you are away for a given period of time and direct the sender to leave a message or forward a copy to one of your counterparts as appropriate.

e. System Access

NIRDA computers that have been out of use shall be automatically updated with the latest antivirus signature file by NIRDA ICT personnel. Users shall terminate active sessions and/or log out of their computers when moving away from the workstation as appropriate. Offices, computer rooms and storage facilities shall always be locked when unattended. In addition, all users shall be responsible for the safety and custodianship of the ICT equipment in the office and outside the office

8. CYBER SECURITY

Users must take note that they share the responsibility of physical and logical security of ICT equipment and data, thus they are required to report any misuse of ICT equipment and data but also alert the NIRDA ICT personnel of potentially relevant threats. It is the user's responsibility to seek guidance from NIRDA ICT personnel when in doubt of what constitute acceptable or prohibited use of ICT equipment and data.

The NIRDA ICT personnel shall put in place mechanism to ensure security of information within the institution. This includes:

- Cyber security awareness
- Establish role-based controls
- In conjunction with RISA, NIRDA shall perform regular vulnerability assessment and penetration testing

a. Cyber security awareness

The NIRDA ICT personnel must plan and conduct regular (at least once a year) cyber security awareness for all end users across NIRDA and affiliated agencies.

b. Role based controls

The NIRDA ICT personnel shall maintain a list of all its interested /relevant ICT stakeholders within and outside the organization. This list shall include role, needs and expectations of stakeholders shall continuously be updated.

c. Regular vulnerability assessment

The NIRDA ICT personnel shall together with the Datacenter under supervision of RISA perform ICT vulnerability and penetration testing at least once a year.

The NIRDA ICT personnel should be prepared to mitigate or respond as quickly as possible to a cyber-incident which can hit institution's IT infrastructure and shall ensure that a proper disaster recovery plan has been put in place to ensure business continuity while recovering from such incident.

Users shall use strong password (combination of lowercase, uppercase, numbers and special characters) with minimum 8 characters in length.

Password shall not be written down, easy to guess and shared to anyone.

Users shall not include password in any automated logon process, e.g.: stored in a macro or function key.

Users shall change temporary passwords at first logon and ensure that nobody is watching when the password is being entered.

Users shall change passwords at regular intervals 90 days.

User shall change password when there is any indication of possible system or password compromise.

Users shall avoid reusing or cycling old passwords.

Windows Sessions shall be logged off after a very short time of inactivity and require the password to be re-entered.

Critical ICT Facilities and services managed by NIRDA shall be restricted to authorized staff by using passwords, locks or access control devices. These facilities include but may not be limited to computer room, ICT server rooms, network and communication rooms.

Third parties such as cleaning staff, internees, external technicians shall access such areas only under authorization of the NIRDA ICT personnel. Details of third parties including names, time out and reason for entry among other shall be recorded.

An appropriate alarm system must be installed in the computer facilities such as, server room.

Human friendly fire prevention (Fire extinguishers) and fire detection systems shall be installed in the computer facility rooms and shall be regularly tested by ICT team.

9. ICT HARDWARE AND SOFTWARE ACQUISITION

Any ICT equipment or software acquisition must pass through framework contract signed between RISA and suppliers on behalf of government institutions or request a non-objection from RISA.

a. Hardware acquisition

- The NIRDA ICT personnel shall design and circulate ICT needs template to all departments for consolidation and approval by DAF.
- Validated ICT needs list shall serve as institutional ICT needs for funds mobilization.
- Terms of references and/or Technical specifications shall be provided by user department in collaboration with the NIRDA ICT personnel for digitalization office consultation, mobilizing fund and facilitate the tendering process.
- Hardware purchased through procurement process shall be in accordance with the Rwandan Public Procurement law, policies, regulations and procedures.
- The NIRDA ICT personnel shall be consulted in all procurement of ICT equipment and software.
- Equipment acquired shall be inspected and approved by the NIRDA ICT personnel and receiving committee for compatibility during the acquisition process.
- Ergonomic or comfort design factors shall be taken into consideration and must be in line with regulatory requirements.

b. Software acquisition

- The acquisition of software and licensing shall be acquired based on the Rwanda Procurement Laws and guidelines, except for donor-funded that may state otherwise.
- Software to be purchased shall be licensed and the NIRDA ICT personnel has the mandate to ensure that licenses of software running on computing devices are still valid.
- Software acquired through any processes shall be inspected and approved by the NIRDA ICT personnel in collaboration with digitalization office for compatibility during the acquisition process.
- Notification to the Digitalization Office shall be made upon delivery to facilitate the installation of new supplied software to the NIRDA's computing devices.
- No shareware or freeware and open-source software shall be loaded into NIRDA ICT assets without written permission from DAF.
- The NIRDA ICT personnel shall ensure that all software that are running on NIRDA's computing devices are updated.
- The installation of update on computing devices shall be managed by the NIRDA ICT personnel.
- The software shall be uninstalled from NIRDA's computing devices in case its license expires and there is no need to renew it.

10. BACKUP AND DISASTER RECOVERY (ON-SITE AND REMOTE BACKUP)

- The NIRDA ICT personnel shall ensure taking backup regularly.
- Performed backups shall include, at a minimum critical databases' master files, transaction files, critical applications, configuration settings and user documentation.
- The backup shall be encrypted with password or pin.
- Backup media shall be clearly labelled, prevented from overwriting, appropriately stored and protected in transit e.g., in secure containers.
- Backups of sensitive data shall be protected in accordance with the GoR Information classification scheme e.g. encrypted when necessary.
- Backups shall be regularly checked to determine whether recovery is possible.

11. CONFIDENTIALITY

- All maps, drawings, photographs, mosaics, plans, manuscripts, records, reports, recommendations, estimates, documents and all other data (referred to hereinafter in this Article as "documents") compiled by or received by the contractor or its agents, servants, employees, subcontractors or independent contractors in connection with a given contract/agreement shall be the property of the NIRDA, shall be treated as confidential and shall be delivered only to duly authorized NIRDA's officials on completion of work or services, or as may otherwise be required by NIRDA.
- In no event shall the contents of such documents or any information known or made known to the contractor by reason of its association with NIRDA be made known by the contractor or its agents, servants, employees, subcontractors, or independent contractors to any unauthorized person without the written approval of the Client.
- Subject to the provisions of this policy, the contractor may retain a copy of documents produced by the contractor.
- The contractor shall take all reasonable measures to ensure that its agents, servants, employees, subcontractors, and independent contractors comply with the provisions of this policy.

12. COMPLIANCE

- This ICT Policy applies to NIRDA devices and systems, as well as privately-owned devices using NIRDA networks and resources. The policy applies to technology administered by individual departments and by authorized resident visitors on their own hardware connected to the NIRDA network

- Breach of this policy may result in disciplinary action in accordance with the NIRDA Disciplinary Policy and Procedure. Any breach of the law will be reported to the appropriate authorities.

13. IMPLEMENTATION AND MONITORING OF THIS INTERNAL ICT POLICY

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

14. APPROVAL OF INTERNAL ICT POLICY

The internal ICT Policy shall be approved by NIRDA Senior Management and shared to Digitalization office.

15. REVIEW

This policy will be monitored by the Administration and Finance unit to ensure it is fit for purpose and reviewed every 2 years and whenever it is deemed necessary. Any change shall be approved by NIRDA Senior Management.

ANNEXES TO THE ICT POLICY

1. Annex I: Policy Acknowledgement for the ICT Policy
2. Annex II: Laptop (Portable Device) Acceptable use and permission form
3. Annex III: Good Practice Guide

ANNEX I: POLICY ACKNOWLEDGEMENT FOR THE ICT POLICY

In effect: ...../...../..... until further notice

I have read, been informed, and understood about the content, requirements, and expectations of the policy for employees at the National Industrial Research and Development Agency (NIRDA). I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment and my continuing employment at NIRDA.

I understand that if I have questions, at any time, regarding this internal ICT Policy, I will consult with my immediate supervisor and the Director of Administration and Finance(DAF).

Please read the Internal ICT Policy carefully to ensure that you understand the policy before signing this document.

Employee Signature: _____

Employee Name: _____

Date: _____

ANNEX II: LAPTOP AND OTHER COMPUTING DEVICES ACCEPTABLE USE AND PERMISSION FORM

The intent of this contract is to insure that laptops users will comply with all acceptable use policies and be informed of liability if laptops are lost, stolen or damaged when used for NIRDA official duties (being in NIRDA premises or outside).

In exchange for the use of laptop computers at work or at home, I understand and agree to the following:

A. NIRDA ICT Policy will be followed when using the laptop and other computing devices at home or at work.
B. NIRDA official duty is defined as the work officially assigned to the employee by her/his supervisor in the interest of the institution.
C. NIRDA reserves all rights to any files or programs that are stored on the laptop and will remove any material which the Standards Board, at its sole discretion, believes is illegal, pornographic, obscene or otherwise objectionable.
D. Users may lose the privilege of using a laptop computer and other computing devices if any of the above policies are broken and or they abuse the equipment, download objectionable material, hack or modify programs or system files without permission or purposely infect the computer with a virus.
E. The staff to whom the laptop and other computing devices are allocated is liable for all damages and repairs that are not normal wear of the computer. He/she is also liable for replacement cost if the laptop and other computing devices are lost or stolen in accordance with articles: 10, 11, 12, and 13 of the "Presidential Order No: 65/01 of 04/03/2014" determining modalities of imposing disciplinary sanctions to public servants.

The following procedure will be followed when allocating laptops and other computing devices to an employee:

1. The employee must be informed on the laptop identification and other peripherals devices before receiving it.
2. The employee must sign and have a copy of NIRDA ICT Policy and Laptop Acceptable Use and permission form agreement before allocating a laptop and /or other computing devices.

I agree with and am willing to follow the above and understand that I am liable if it is lost, stolen or damaged.

Employee Signature _____ Date _____

Employee Names: _____

MUNYAZIBONEYE Emmanuel
Director of Administration and Finance

By the delegation of authority:

.....

Logistics Officer

.....

Laptop Identification (NIRDA Tag number): .....

Brand and Model	Serial Number	Battery SN:	Accessories			Observation
			Item name	Specification	Quantity	

ICT EQUIPMENT AND COMPUTING DEVICES SUBMISSION FORM

Names: .....

Department/Unit: .....

Date: ...../...../.....

SN	ITEM NAME	Serial number	Barcode	Asset status

ANNEX III: GOOD PRACTICE GUIDE

Below is a summary of recommended Do's and Don'ts for all users of NIRDA ICT systems. It is intended to complement approved NIRDA policies and support new information governance standards set by different divisions in NIRDA.

DOs

- Do ensure you keep security in mind when working – If you have been sent a file or a web link, are you sure you can trust the person it came from, is this the type of thing they would normally send, does it 'feel right'? Remember, lots of spam and viruses sent impersonate the e-mail address of a real person, so the e-mail may not have been sent by the person you think. Lots of viruses move from machine to machine as hidden files on storage devices. Remember, only IT equipment issued, or approved, by the ICT Personnel should be used.
- Do report any errors or problems promptly – If you have an error or an issue, especially if it may be security related, please report it to the ICT Personnel quickly and with as much detail as possible. Reporting that you had a problem 3 days ago and you can't remember the error message makes it almost impossible to track and correct the problem. Reporting promptly with details of which system (e.g. server, e-mail) was affected, the date and time the problem occurred and the specific error message or event makes it much easier to find and fix the problem, and get you working again.
- Do think about what you are saving and copying onto the network and in e-mail. Does the file need to be there? How big is it? If you are saving an attachment out of an e-mail, remember to delete the copy in the e-mail to save using up double the space. If you are

copying data from a DVD, why is this necessary? If it is only for your use, can it stay on the DVD?

- Do take care of the equipment you are issued with, either permanently or on loan. Most of it is expensive and it may contain sensitive or confidential data.
- Do remember to return the equipment before leaving NIRDA. All data will be securely erased by the NIRDA ICT personnel. Please note that any personal data that has not been erased from returned equipment may be viewed by the Administration and Finance Directorate.
- Do keep passwords secure and never disclose them to anyone else. Passwords should ideally contain at least 9 characters with a mix of letters and symbols in upper and lower case.
- Do keep portable media, especially laptops, taken outside NIRDA offices secure at all times. For example, do not leave them in boots of cars overnight, in overhead luggage racks or unattended in other insecure areas. Where possible carry IT equipment in anonymous cases without a manufacturer's logo and avoid using laptops in public places where possible if confidential information may be visible to other people.

DON'Ts

- Don't connect any equipment (Laptops, USB devices including storage devices, networking equipment, cards for any kind of generation of wireless mobile telecommunications technology, etc.) to NIRDA ICT systems unless it has been supplied or specifically authorized by the NIRDA ICT personnel. If in any doubt, confirm with the Office before connecting anything.
- Don't download any Software, Software updates, Installation Packages, or Executable files from the Internet or external storage devices (USB sticks, external hard drives, CD-ROM, DVD etc.) onto NIRDA ICT systems unless specifically authorized by the NIRDA ICT personnel.
- Don't install any software on any NIRDA ICT systems unless specifically authorized by the NIRDA ICT personnel. All software installs are normally carried out by the NIRDA ICT personnel and user installation of software is only authorized in special circumstances.
- Don't download, upload, store, copy or distribute any materials, data or software of a pornographic, obscene, indecent, racist, defamatory, libellous, sexist, offensive or otherwise unlawful nature (other than for properly authorized and lawful research, for which written notification must be given to the relevant Director).
- Don't attempt to circumvent the security and restrictions in place on the NIRDA ICT systems. These are in place to ensure a safe working environment for all staff and maintain the security and resilience of the NIRDA network.
- Don't leave portable media unattended in public places where there is a potential for opportunist theft or compromise (i.e. installation of a virus).

- Don't connect any NIRDA issued equipment or storage devices into another computer or network unless you are happy the network is correctly maintained and up to date Anti-Virus protection is in place. Viruses can be transferred using machines and storage devices connected to compromised computers or networks.
- Don't use the NIRDA network, including U drives, for the storage of music files, as these may breach copyright permissions. Private photographic and or video files should not be stored on U drives as they use up large amounts of space.

For further information and advice please contact the NIRDA ICT Personnel or log an IT Support request through support email: ITsupport@nirda.gov.rw

Done at Kigali 18th January 2023