REPUBLIC OF KENYA

NATIONAL RESEARCH FUND

ICT POLICY

May 2023

DOCUMENT NAME, OWNERSHIP AND VERSION CONTROL

Original Issue Date:	**17th April 2023**
Responsible Executive	Chief Executive Officer
Owner	Chief Executive Officer
Contact Person	Director, Corporate Services
Classification	ICT Division
Functional Applicability	National Research Fund
Preparation Date	2023
Next Review Date	2024
Version	ICT Policy
Document Storage	Document Management System

DOCUMENT REVIEW

ACTIONS	RESPONSIBLE	SIGNATURE & DATE
Controlled By:	Chief Executive Officer	 **22/06/2023**
Approved By:	Chairman, Board of Trustees	 **30/06/2023**

Table of Contents

Executive Summary

In today's digital age, information and communication technology (ICT) play a critical role in the operations of organizations across industries. The use of ICT has become integral to the success of businesses, and as such, it is essential to have policies that govern its use. The NRF ICT Policy is a comprehensive document developed to guide the use of ICT within the organization and ensure the security of its information and assets.

The policy outlines the NRF's commitment to providing a secure and efficient ICT infrastructure, promoting the responsible use of ICT resources and ensuring compliance with all relevant laws and regulations. The policy covers several areas, including hardware and software usage, internet and email usage, data security, privacy among others.

The policy includes several components, including guidelines for the proper use of ICT resources, protocols for data security and privacy, and procedures for reporting and handling ICT-related incidents. The guidelines for the proper use of ICT resources aim to promote responsible and efficient use of ICT resources, while the protocols for data security and privacy aim to ensure the protection of confidential information and assets.

The policy is designed to comply with all applicable laws and regulations related to ICT as it aligns with the NRF's values of accountability and transparency, as well as its commitment to creating a safe and secure work environment.

The approval of this policy demonstrates the Board's commitment towards supporting responsible use of ICT resources, the protection of confidential information, and compliance with all relevant laws and regulations.

Ratemo W. Michieka, Professor Emeritus PhD., EBS, SS.
Chairman, Board of Trustees

Foreword

In today's rapidly changing technological world, nanotechnology era and networked organizations are the order of the day and developing institution-wide network systems requires policy framework. The National Research Fund has developed this Policy in line with the National Agenda towards the attainment of Kenya Vision 2030 through an industrialized information society and knowledge economy. The objective of this policy is to allow greater innovation and future thinking in the implementation of the NRF mandate.

Information and Communication Technology (ICT) services are today a critical pillar to the operations of all funding institutions. Deploying reliable and efficient ICT services and operations can be achieved if there exists an ICT Policy which guides and commands the execution of different procedures regarding the institution's ICT master plan, vision and mission.

This ICT Policy sets the direction for the National Research Fund by providing a framework for the use and management of its ICT resources. The National Research Fund therefore, affirms its commitment to adopt and operationalize e-Government standards; ensure availability of internet bandwidth within the institution ICT infrastructure; ensure that anti-virus updates, data back-up are in place; increase the percentage of staff who have access to broadband and Internet in the work place.

Prof. Dickson Andala
Chief Executive Officer

Definition of Terms

"**ICT**" in this policy refers to all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are owned, controlled, or operated by the Fund. It includes but it is not limited to; computers (such as desktops, laptops, PDAs,), computer systems, storage devices (such as USB and flash memory devices, CDs, DVD, iPads, MP3 players) imaging devices (such as photocopiers, scanners, cameras, CCTVs), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), telecommunication equipment (such as PABX, fax machines, telephone terminal sets, IP-phones), computer networks, databases and any other similar technologies as they come into use.

"**User**" means anyone who operates or interfaces with ICT. It includes Fund staff, officers or any other member of the Fund.

"**Authorized User**" means a member of the Fund staff allowed to use ICT resources.

"**Copyrighted content**" means material for which the copyright for the content is held by a third party other than the National Research Fund e.g. music, computer software, films, video.

"**P2P Application**" is software running on device to provide the communications of file sharing capabilities between peers. This software is usually downloaded from the Internet and includes but not limited to applications such as Kaaza, BitTorrent and LimeWire.

"**Fund**" refers to the National Research Fund.

List of Acronyms

CD	-	Compact Disk
DVD	-	Digital Video Disk
ICT	-	Information & Communication Technology
ISP	-	Internet Service Provider
KENET	-	Kenya Education Network
LAN	-	Local Area Network
NRF	-	National Research Fund
SMTP	-	Simple Mail Transfer Protocol
WAN	-	Wide Area Network
WWW	-	World Wide Web
EMS		Electronic Messaging Service
DICT	-	Division of Information & Communication Technology
DCC	-	Division of Corporate Communication
P2P	-	Peer-to-Peer
PC	-	Personal Computer

1.0 Introduction

The National Research Fund is in the process of scaling up its ICT resources and services. The increasing number of staff and clients in need of accessing ICT services has necessitated the increase of the number of computers as well as upgrading networking infrastructure. This policy once approved shall help NRF in establishing a scalable, sustainable, effective, manageable, and optimal ICT hardware and software infrastructure. It will also guide in the acquisition, continuous development, administration, maintenance, and usage of the ICT devices.

1.1 Policy Objectives

1.1.1 General Objective

To support the business functions of NRF by improving operational productivity and innovativeness so as to improve customer and user satisfaction.

1.1.2 Specific Objectives

The specific objectives of NRF's ICT policy are to:

1. To provide accessible, affordable, reliable, secure and quality ICT facilities and services.
2. To create an enabling and conducive environment for the improvement of customer and user satisfaction.
3. Support innovative and effective ICT for efficient service and information delivery.
4. Help people to adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT.
5. Promote information sharing, transparency and accountability and reducing bureaucracy in operations.

2.0 The Policy Framework

The following policy statements provide a foundation for the development of the specific ICT policies that will be developed as the need arises. Such policies may include but are not limited to the following:

1. ICT Services Management Policy
2. ICT Acceptable Use Policy
3. Software Acquisition and Installation Policy
4. ICT Malware Policy
5. Password Policy
6. Website Policy
7. ICT Systems Security Policy
8. Email Policy
9. End User Support Policy

10. Internet Usage Policy
11. Help Desk Triage Policy
12. Backup Policy
13. Business Continuity Plan

2.0.1 Related Policies and Information Sources

NRF recognizes that ICT is a management discipline and as such will be managed as an ongoing cyclic process with due consideration to this policy. The policy is based on the following Legislation and reference guides:

a) Public Procurement and Asset Disposal Act Revised Edition 2016
b) Data Protection Act, 2019
c) Computer Misuse and Cyber Crimes Bill 2018
d) The Kenya Information and Communication Act 2009 COBIT 5 Framework
e) ITIL Framework
f) ICT Authority Standards
g) Cloud computing standard
h) Data Centre standard
i) Electronic records and data management standard
j) End-user equipment standard
k) Information security standard
l) IT governance standard
m) ICT network standard
n) Systems and applications standard
o) NEMA draft E-Waste regulations

By adopting elements from these references, this ICT policy is suited to the specific nature of NRF's mandate while adopting the world's best practices.

2.1 References

i. National Information and Communication Technology ICT Policy
ii. Other applicable policies

2.2 Appendices

The specific ICT policies development based on the policy statements are hereafter appended. The following are the ICT Policy Appendices based on the policy statements.

3.0 Appendix 1: ICT Services Management Policy

3.1 Introduction

Information processing and communication services form vital resource to NRF that must be carefully planned, deployed and maintained. Structure to plan, organize and coordinate such services and policies that govern them must, therefore, be put in place.

3.2 Purpose

This policy defines the governance structure of ICT functions at NRF.

3.3 Scope

This policy shall govern the management structure of the ICT services at NRF.

3.4 Role of Management

i. Shall ensure that ICT policy decisions are realistic and focus on improving institution's service delivery.
ii. NRF shall establish a Division of ICT (DICT), which shall be responsible for managing and maintaining ICT systems and end-user support.

3.5 Role of DICT

The NRF shall provide ICT services to all users and actively offer professional training.
The specific functions of DICT shall be to:

i. Provide computer services through sustainable automation of all information generation, processing, and communication operations,
ii. Design, develop and implement viable state-of-art systems,
iii. Ensure a well-maintained and up-to-date ICT infrastructure,
iv. Ensure that staff can adequately make use of modern ICT technologies by providing demand-driven ICT training,
v. Undertake research, development, innovations, and technology transfer.
vi. Provide technical support to the ICT Committee in the formulation of ICT policy guidelines and regulations.

3.6 Resource Ownership

Each ICT device (computer, data communication device, software, network components, and data storage), must have a defined owner The management shall determine ownership of specific ICT devices.
All in-house developed software systems shall remain a property of NRF and no person has the right to copy or distribute such software systems to other parties.

3.7 Service Level Agreements (SLAs) and Service Charters

DICT shall ensure the smooth running of quality services through engaging Service Level Agreements (SLAs) and signing Service Charter with its clients.

4.0 Appendix 2: ICT Acceptable Use Policy

4.1 Introduction

This policy informs NRF's staff and other individuals entitled to use its facilities of the regulations relating to the use of Information Communications Technology systems.

4.2 Purpose

The purpose of this policy is to:

i. Define the guiding regulations on the usage of ICT facilities at NRF.
ii. Protect the privacy and integrity of data stored on the ICT equipment.
iii. Encourage users to understand their own responsibility for protecting NRF's ICT equipment.

4.3 Scope

This policy shall regulate the usage of ICT facilities at NRF.

4.4 Policy Statements

i) NRF requires that all people exercise due care and attention over their use of ICT facilities. This shall apply to the direct (NRF facilities) and indirect (third-party equipment connected to NRFs facilities) use of NRF's ICT facilities.
ii) All software on any equipment connected to NRF's ICT facilities shall be properly licensed, and the terms of the license be strictly observed.
iii) Users will not access, interfere, or remove any ICT facility or data or information unless they have been authorized to do so.
iv) Users shall use ICT facilities in a manner that is consistent with their role.
v) Users will not use ICT facilities in such a way as to deliberately disrupt or interfere with the use of those facilities by others.
vi) All use of ICT facilities shall be lawful, honest, and decent and have regard to other people's rights and sensitivities.
vii) Users shall not deliberately create, use, or distribute materials that could bring NRF into disrepute.
viii) Duly authorized officers of NRF may access or monitor electronic data held on or transiting NRF ICT facilities where there is a belief that the individual may be in breach of NRF regulations or the law, or where required to do so by an external agency, e.g., the Police, or where individuals are absent and no arrangements have been made to allow access to information crucial to the working of NRF.
ix) The Holder of a computer account, computer system, or any system account connected to NRF is responsible for the actions associated with the computer account or computer system.
x) Users shall be expected to assist ICT support staff with investigations into suspected violations or breaches of security.
xi) All NRF's Computers shall have working surge-protected UPS which will be tested from time to time.

4.5 Enforcement

Individuals in breach of this policy are subject to disciplinary procedures established for staff discipline.

5.0 Appendix 3: Software Acquisition and Installation Policy

5.1 Introduction

As software applications are purchased and as updated versions of currently supported software are released, installers shall be updated manually by DICT or automatically via the Internet. The DICT shall purchase, install and track licenses for NRF software acquisitions.

5.2 Purpose

This policy has been established:

i. To ensure that all users understand and agree to abide by specific software, program, and application acquisition and installation guidelines, and use on organization-provided computers, systems, and networks.
ii. To set out guidelines, governance, code of practice and acceptable use of software in the staff's PCs connected to network.
iii. Ensure all IT equipment and software at NRF is procured in the most cost-effective way and meets minimum NRF operating standards.

5.3 Scope

This Policy shall apply to all the computing facilities of NRF. The policy shall not be extended to cover installation on non-NRF owned hardware or unsupported operating system.

5.4 Appropriate use of software

i) **Copying of Software**: Users shall not allow NRF's licensed software and/or associated documentation to be copied by outsiders and may not themselves make copies other than those provided for in the relevant licensing agreements.
ii) **Application Development Approach**: Standard Software Development Lifecycle (SDLC) methodology shall be applied to planning, analysis and design as well as management and implementation of custom-built software.
iii) **Software Configurations**: Software configurations shall be documented for easier reference.
iv) **Authorized Software**: Authorized software is considered to be software that meets the following conditions:
    a. The software is used in accordance with license terms;
    b. The software has been tested by an authorized DICT Officer to ensure functionality and security of ICT Facilities;
    c. The software has been installed by an authorized DICT Officer; or
    d. The installation of the software has been authorized by an DICT Office
v) **Unauthorized Software:** Unauthorized software is considered to be any software that:
    a. Is used in breach of software license agreements;
    b. Has not been tested by an authorized DICT Officer;

c. Is not installed by an DICT Officer; or
d. Has not been authorized by DICT Officer.

vi) **Unlicensed or Pirated Software**: Unlicensed or pirated software is considered to be all software used outside of the license agreement that accompanies the software.

a. The use of unlicensed or pirated software on NRF's ICT facilities is strictly prohibited,
b. Any person cannot authorize the installation and use of unlicensed or pirated software. The software shall not be installed or used until the conditions of the license have been met.
c. Any software installed or used in violation of license terms shall be deemed unauthorized software and will be in breach of this policy.

5.5 Software Installation

This policy is established to cover the following areas:

a) Access and Availability
b) Software Use
c) Security
d) Management and Monitoring
e) Advice and Assistance

5.5.1 Access and Availability

i) **Standard Operating Environment**

DICT shall develop, maintain and publish a Standard Operating Environment (SOE) for the use of NRF's computing equipment.

ii) **Mandatory Software**

a. DICT reserves the right to install mandatory software on all computing equipment.
b. All NRF's computers must have anti-virus software, automated updates and remote support utilities.
c. All requests for the installation of software must be made through DICT.
d. DICT shall provide software installation to NRF workstations for administrative use only.

5.5.2 Software Use

A user must abide by all software license agreements. NRF is committed to ensuring that the use of software abides by all relevant legislation.

a) **Software Installed/Stored on Shared Resources**

i. Software cannot be placed on a server or a network where it would be available to non-licensed users for use or copying.
ii. Unauthorized placement of software on a network or server may allow a breach of copyright or license agreement.

b) **Uploading or Downloading Unauthorized Software**

i. The staff shall not download or upload unauthorized software over the Internet as it is a breach of the Copyright.

c) **Software used for Commercial or Profit activities**

ii. NRF's staff are not permitted to use NRF's software for personal business or personal gain.

d) **Personally Owned Software**

i. Personally owned software shall not be installed on NRF equipment unless authorized by DICT.

ii. Licenses for such software must be kept with the equipment, upon which it is being used, at all times.

5.5.3 Security

i. DICT will keep all software master copies and license certificates in a secure location and will only be accessible to authorized personnel.

ii. In the case of individually licensed software, the license must be located with the equipment.

5.5.4 Management and Monitoring

i. For the purpose of compliance with copyright legislation and licensing agreements, NRF reserves the right to audit and remove software from any of the NRF-owned computers.

ii. The staff on learning of any misuse of software or related documentation within NRF shall notify their Head of Work Unit and/or the head DICT.

iii. The staff have an obligation to help ensure that NRF does not become involved in any possible copyright or license breaches.

iv.

5.5.5 Software Installation Request Procedure

i. Any request for the installation of software onto NRF servers or workstations for staff usage must abide by the following criteria:

   a. The full installation package (CD-ROM, zipped or self-extracting files, etc.) along with the installation manuals must be delivered to DICT.
   b. DICT staff must have all available resources, authority and time necessary to complete any software installation.

5.5.6 Delivery of Installation Request

ii. NRF staff must follow the following criteria for any request to have software installed in order to avoid time delays and other potential obstacles.

   a. Indicate to the requestor an estimated date of delivery.
   b. Arrange a time for the requestor to test the software.
   c. Provide a brief user guide on locating the software, which users are authorized to access and use, and how the software is installed and configured.
   d. Ensure that the testing is conducted in a lab environment using relevant PC's or Macintosh's and including printing. At this stage, all access to the software is restricted to testers.

e. Once the request has successfully tested the software, the staff will ensure that the requestor completes a Software Applications Acceptance Testing form.
f. When acceptance testing and acceptance is completed, the software will then be released for use by the target audience.

5.5.7 Post Acceptance Testing Issues

a) Software Failure

i. The requestor is to notify DICT in writing of any failure of a software component after acceptance testing.
ii. DICT staff will indicate an approximate time for assessment of this job after considering the urgency and other priorities.
iii. Failure of installed software must be considered as a new job since a remedy may require considerable time and resources

b) Installation of Extra Modules of Previously Installed Software

i. The installation of new modules of previously installed software is to be considered as a new job request and will follow the same guidelines.
ii. New modules of software can require the same amount of time and planning as new software.

c) Changes to Client Software

i) All changes to client software must be reported to DICT for licensing and audit purposes.
ii) A license installed in a PC or Laptop, shall be transferred to another user if the former staff member leaves NRF.
iii) It is the responsibility of Divisions to inform DICT of any changes to client software by contacting DICT.

5.5.8 Return of ICT hardware, software and electronic devices

a. ICT hardware, software and electronic devices shall be returned on termination of employment.
b. Arrangements for the return or redistribution of hardware, software and electronic devices shall be made with consultation with Asset Management.

6.0 Appendix 4: ICT Malware Policy

6.1 Introduction

Institutions are increasingly dependent upon the usage of ICT network(s) as a key tool for conducting their core mandate. A major threat to the delivery of ICT services is malicious software (malware) which has the potential to undermine the confidentiality, integrity and availability of those/data hosted on ICT systems or can adversely impact the underlying infrastructure hosting these systems and thus prevent access to the resources.

ICT Division is responsible for ensuring that appropriate technical measures are implemented to protect against malware and that appropriate controls are in place to rapidly detect, isolate and remove any instances. However, a single technological solution cannot be relied upon. Therefore a 'layered approach' will be implemented to provide the best overall protection against the omnipresent threat of malware from whichever vector it may appear.

6.2 Purpose

This policy has been established to:

i. Minimize the risk of Malware infections to NRF's ICT facilities and services.
ii. Ensure the integrity of NRF's ICT facilities and services.
iii. Ensure reliability and availability of NRF's computing devices.

6.3 Scope

This policy applies to ICT resources and all NRF employees authorized to use/access those computing systems and communication networks whether they are employed directly by the trust, contractors, voluntary organizations or suppliers granted access for support purposes. It is the personal responsibility of each individual to take precautions to ensure that all forms of malware are not introduced into any of NRF's resources or system with which they come into contact.

6.4 Virus Management General Policy

i. All ICT equipment will have appropriate active malware protection. The most current version of the anti-virus software package will be taken as the default standard and installed in the NRF's Application Server.
ii. Any activities to create and/or distribute malicious programs onto NRF network are strictly prohibited.
iii. If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the DICT immediately.
iv. Users shall never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
v. Users shall avoid direct disk sharing with read/write access. Always scan a flash disk for viruses before using it.
vi. Users shall back up critical data and systems configurations regularly and store backups safely.

6.5 DICT's Responsibilities

The DICT shall:

i) Employ virus management measures at appropriate points of NRF network.
ii) Implement virus control software and procedures to ensure that all networked computer servers and ICT-managed workstations have protection against virus infection.

iii) Immediately disconnect compromised ICT facilities and services from NRF network until a remedy process is complete.

iv) Not connect to NRF network computer equipment owned or leased by users, without appropriate and maintained anti-virus software.

v) Disconnect from NRF network any user owned or leased equipment that does not have appropriate and maintained anti-virus software installed.

7.0 Appendix 5: Password Policy

7.1 Introduction

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of NRF's resources. All users with access to NRF facilities and services shall comply with this policy's minimum standard for passwords.

7.2 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides in NRF, has access to NRF's network, or stores any non-public information.

7.3 Purpose

i. To ensure appropriate password controls are implemented that address the risk of unauthorized access to the various ICT facilities and services at NRF.

ii. To establish a minimum set of password management controls which apply across DICT facilities and services at NRF as a baseline requirement.

iii. To establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

7.4 Minimum Standard for Password

Minimum Length of password	8 characters (Alphanumeric, alphabets, special characters and numbers)
Number of unsuccessful logins attempts before the username is made inaccessible automatically (locked)	3 Times
Duration of the lockout period	60 Minutes (Router) 30 Minutes (User PCs)
The period after which a password must be changed	120 Days (every 4 months) - Users can change their own passwords at any time
Reusability of old passwords	Users will not be allowed to use a password they have used before within the last 4 months

Users shall:

i. Keep passwords secure and shall not share accounts. Authorized users are responsible for the security of their passwords and accounts.
ii. Not write the password down in an insecure location.

8.0 Appendix 6: Website Policy

8.1 Introduction

NRF runs a website to provide information on its core mandate. Through the website, several services are made available to staff. This policy outlines the structure of the relevant staff, policies, procedures and technical systems that maintain and manage the institution's website.

8.2 Purpose

i. Provide information to NRF staff, affiliate institutions and potential clients.
ii. Provide easy access to NRF press releases and a customized news section.
iii. Reduce duplication of website content, website management and maintenance efforts.

8.2 Scope

This policy governs all web-based activities commissioned by NRF, including public web pages representing offices, schools, Divisions, institutions and centers.

8.3 Roles and Responsibilities

8.3.1 Webmaster

a) The Webmaster shall provide quality assurance on the:
   i) Content
   ii) Look and feel of NRF's Website ensuring that it is in tune with NRF's mission, unique identity, core values and status.
b) The Webmaster shall be responsible for setting policies governing the nature, content, format, maintenance, timeliness and ownership of information on the website's official pages.
c) The Webmaster shall be responsible for updating the website and responding to emails.
d) The webmaster shall be responsible for maintaining the content of the Home and main web pages.

8.3.2 Division of Corporate Communications (DCC)

a) The Division of Corporate Communications (DCC) shall be responsible for maintaining the content of the Home and main web pages.
b) Information to be published on all web pages shall be routed through the office of DCC.
c) The DCC shall proofread, edit, and approve the content for publishing.

8.3.3 Division of ICT

The DICT shall provide technical and advisory support services for the website. In addition, the DICT shall be responsible for maintaining NRF's web server.

8.4 Website Structure and Content

The website shall comprise the following web pages:

8.4.1 Main Web Pages

These shall comprise NRF Home Page and pages that provide:

a) The profile of NRF, *i.e.*, the governance structure, programs of the Divisions/sections, Institutes and centers, as well as the administrative Divisions.
b) Grants announcements, application processes and requirements.
c) NRF Policies and Regulations.
d) News, events and announcements.

8.4.2 Staff Web Portal

This shall be made up of pages that capture the profiles of the staff.

8.5 Website Rules and Regulations

8.5.1 Main Web Pages

- The DICT shall be responsible for updating and maintaining the content of the main Fund web pages.

8.5.2 Websites of Affiliates and Others

i. Links to the websites of Institutions affiliated with NRF or otherwise shall be established at the discretion of NRF.
ii. The DCC shall conduct due diligence on the institution's website using the provisions in this policy document and grant approval in consultation with the Webmaster.

8.5.3 Applications to Link to the Website

i. Outside institutions or organizations that wish to establish a link on their website to that of NRF shall apply to the DCC.
ii. The DCC shall conduct due diligence on the institution and their website using the provisions in this policy document and grant approval in consultation with DICT.

8.5.4 General Guidelines for Web Pages

The following guidelines apply to all web pages under the control of NRF:

i) **Identification**: The NRF logo or logotype shall identify all web pages.
ii) **Contact Information:** All web pages shall carry the Email address of the Division or officer in charge of their upkeep.

iii) **Legal Compliance:** The content on all the pages shall not violate the NRF's policy and statutes, copyright, libel, obscenity or other local or national laws.

iv) **Commercialization:** Web pages shall not be used for commercial purposes, sales or moneymaking ventures except those authorized by the management.

v) **Accuracy and Currency:** All pages shall be accurate, well written, concise, and free of spelling and grammatical errors and shall otherwise present the NRF's mission and values positively.

vi) **Monitoring:** The Web Assistants shall monitor the content on all the pages regularly to ascertain that material is current or appropriate. Outdated or inappropriate materials shall be removed within two working days when they are noticed.

8.5.5 Enforcement of Website Policy:

a) Any staff or individual that notices an error or considers content on the website inappropriate may bring it to the attention of the DCC or Web Assistant in charge of the page.

b) The DCC or Web Assistant shall take measures to address the concern and give feedback to the complainant.

c) The following shall govern the escalation procedures if the issue has far-reaching implications:
   - Head/Secretary/Web Assistant of a Division shall escalate to DCC.
   - DCC escalates to Webmaster.
   - Webmaster escalates to Head of DICT.
   - Head of DICT escalates to ICT Management Committee.

d) Where an individual who reported a problem on the site is not satisfied, the complaint shall be escalated to the management.

e) The DCC or the Webmaster may immediately remove any page on NRF website that violates this policy.

9.0 Appendix 7: ICT System Security Policy

9.1 Introduction

NRF plans to invest substantially in ICT resources to meet its business operations effectively. This policy establishes general guidelines, rules and regulations for using and protecting the NRF's information and ICT systems. Implementing this policy will thus promote the availability, integrity and confidentiality of NRF's ICT systems.

9.2 Purpose

This policy has been established to provide guidelines on mechanisms that shall be in place to protect all information technology resources at NRF. The policy mandates all users of NRF's ICT resources to ensure protection procedures are in place to guard such resources against accidental or deliberate, unauthorized alteration, destruction, delay, theft, access, use or damage to systems, data, applications, equipment, and telecommunications.

9.3 Scope

This policy shall be applicable to all organizational units of NRF and any user, contractor, and sub-contractors who shall be involved in developing systems, obtaining, transmitting, using, and processing NRF information and data, on behalf of NRF. This policy shall also apply to NRF's ICT systems operated on behalf of NRF by private organizations to accomplish NRF's function. Lastly, it includes anyone involved in the design, development, acquisition, installation, operation, maintenance and use of NRF's telecommunications, LANs, and WANs.

9.4 General Use and Ownership Policy

i) While DICT is committed to providing a reasonable level of privacy, the DICT shall not guarantee the confidentiality of personal information stored or transmitted on any network or device belonging to NRF.

ii) The data created and transmitted by users on the ICT systems shall be treated as property of NRF.

iii) The DICT shall protect NRF's network and the mission-critical Funds data and systems.

iv) Users shall exercise good judgment regarding the reasonableness of personal use of ICT services. They shall be guided by ICT policies concerning personal use of ICT Internet, Intranet or Extranet systems. In the absence of or uncertainty in such policies or uncertainty, they shall consult the relevant DICT staff.

v) DICT shall continuously monitor equipment, systems and network traffic as provided in the network and development policy.

vi) The DICT shall reserve the right to audit networks and systems periodically to ensure compliance with this ICT Policy.

vii) All network equipment must be physically secured. For example, access to data centers, telephone wiring closets, network switching rooms, and other areas containing Confidential information must be physically restricted.

9.5 Securing confidential and proprietary information

i) NRF data contained in ICT systems shall be classified as either confidential or non-confidential. Examples of confidential information include but are not limited to: payroll data, human resource data, health records and research data. Employees shall take all necessary steps to prevent unauthorized access to confidential information.

ii) All employees who must keep Confidential information offsite to do their work must possess lockable furniture to properly store this information. At the time of separation from NRF, all Confidential information must be returned immediately.

9.6 Wireless Network Users

i) Any person attaching a wireless device to NRF network shall be responsible for the security of the computing device and any intentional or unintentional activities arising through the network pathway allocated to the device.

ii) NRF accepts no responsibility for any loss or damage to the user device resulting from the connection to the wireless network.
iii) Wireless network users shall have proper configuration done on their computer systems to avoid causing inconveniences to the other network users.
iv) Use of NRF's wireless network services for other purposes other than research or related activities is prohibited.

9.7 Confidentiality and Security

i) As NRF's networks and computers are the property of NRF, NRF retains the right to allow authorized ICT officers to monitor and examine the information stored within.
ii) It is recommended that personal confidential material is not stored on or sent through NRF's ICT infrastructure.
iii) Confidential information shall be redirected only where there is a need and with the permission of the originator, where possible.
iv) Users shall be aware that a message is only deleted from the system once all recipients of the message and any forwarded or attached copies have deleted their copies.
v) Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users shall verify authenticity with the DICT.
vi) NRF takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data, nor accepts any liability for consequential loss in the event of improper use or any other circumstances.

9.8 Remote Printing

i. Printers must be supervised if Confidential information is being printed or soon will be printed.
ii. The persons attending the printer must be authorized to examine the printed information.
iii. Unattended printing is permitted if the area surrounding the printer is physically protected, so persons not authorized to see the material being printed may not enter.

10.0 Appendix 8: Email Policy

10.1 Introduction

NRF uses electronic email in almost all its areas of operations as a primary communication and awareness method. The misuse of email can pose many legal, privacy and security risks. Thus, it's important for users to understand the appropriate use of electronic communications.

10.2 Purpose

The purpose of this email policy is to ensure the proper use of NRF's email system and make users aware of what NRF deems acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within NRF's network.

Finally, the policy establishes regulations to ensure users understand their responsibilities when using NRF's electronic messaging services.

10.3 Scope

This policy covers the appropriate use of any email sent from NRF email address and applies to all employees, interns, attachés, vendors, and agents operating on behalf of the NRF. Finally, the policy applies to the use, for the purpose of sending or receiving email messages and attachments, of any ICT facilities, including hardware, software and networks provided by NRF.

10.4 General Policy Statements

i) Only authorized users of NRF's computer systems can use email facilities.
ii) All members of NRF are entitled to always use computing facilities and email systems when the network is available.
iii) NRF complies with and adheres to all its current legal responsibilities, including Data Protection, Electronic Communication, Regulation of Investigatory Powers (RIP), Human Rights, Computer Misuse, Copyright, and Intellectual Property.

10.5 Professional and Ethical Use of Messaging Services

In general, users cannot be protected from receiving offensive electronic messages. The user of NRF's electronic messaging services should act in professionally and ethically. This shall be achieved through the following conditions:

i. Apply the same personal and professional courtesies and considerations in electronic messages as in other communication forms.
ii. Not transmitting messages unnecessarily.
iii. Not transmitting frivolous, ethnic and gender abusive, defamatory messages.
iv. Not transmitting electronic messages that are illegal or contravene other Fund policies.
v. Not disguising the content of the original message.
vi. Not making available any content that they do not have rights to.
vii. Not causing interference with other users of electronic messaging services. Examples of interference include transmission of e-mail chain letters, widespread distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same message.
viii. Not giving the impression that they are representing, giving opinions or making statements on behalf of NRF.

10.6 Personal Use

NRF's electronic messaging services may be used to send or receive incidental personal messages providing that such use will not:

i. Directly or indirectly interfere with NRF's business operations, or
ii. Interfere with the user's employment or other obligations to NRF, or
iii. Cause or be likely to cause damage to NRF's reputation, or

iv. Conflict with any Fund policies, regulations or Kenyan Laws.

10.7 Commercial, for-profit activities or advertisements

i. NRF's electronic messaging services shall not be used for commercial activities or personal gai, except as permitted by other Fund policies.
ii. Advertising or sponsorship is not permitted except where NRF has approved such advertising or sponsorship.

10.8 Email as NRF Property

i. All electronic messages supporting NRF's business are considered to be a Fund record, irrespective of the location or ownership of the facilities used to create or store the electronic form.
ii. Users of electronic messaging services must be aware of their responsibilities regarding the management, retention, and disposal of Fund records.

10.9 Privacy and Monitoring

i. Due to the nature of electronic messaging systems, NRF cannot guarantee the confidentiality of information contained in messages.
ii. System logs might record sender and recipient addresses associated with incoming and outgoing electronic messages.
iii. NRF respects the privacy of users. Therefore, it does not intend to inspect or monitor electronic messages routinely.
iv. It is not the policy of NRF to regularly monitor the content of electronic messages. However, they may be monitored occasionally to support operational, maintenance, auditing, and security and investigate activities. Therefore, users should construct their communications in recognition of this fact.
v. Consent shall be sought by NRF before any inspection, monitoring or disclosure of Fund electronic messages in NRF's possession.

10.10 Inspection of Electronic Messages without Consent

NRF permits the inspection, monitoring or disclosure of electronic messages without the owner's consent only when:

i. It is consistent with and required by law;
ii. There is substantiated reason to believe that violations of law or Fund policy have taken place; or
iii. In exceptional cases, to meet time-dependent, critical operational needs, or
iv. It is necessary to protect the NRF's communication networks.
v. When access to an individual's electronic message is required and is consistent with one of the above items, one of the following may apply.

10.11 Authorization

i. Except in emergencies, such actions must be authorized in advance and in writing by the authority specified by the law or policy under which the action is taken.
ii. If the authority is not specified, authorization must be sought from the appropriate Divisional Head on the advice of DICT.
iii. The advice of NRF's Legal Services should normally also be sought before authorization because of changing interpretations by the courts of laws affecting the privacy of electronic messaging.
iv. At the earliest possible opportunity, NRF shall notify the affected individual of the action taken and the reasons for the action taken unless law or other NRF policy specifically requires otherwise.

10.12 Disclaimer

NRF assumes no liability for direct and/or indirect damages arising from the user's use of NRF's e-mail system and services. Users are solely responsible for the content they disseminate. NRF is not liable for any third-party claim, demand, or damage arising from using NRF's e-mail systems or services. The following disclaimer shall be applied to all outgoing emails:

***DISCLAIMER**: All the information in this email message is strictly confidential and may be legally privileged. Such information is intended exclusively for the designated recipient(s). Any disclosure, copying or distribution of all or part of the information contained herein or other use of or the taking of any action in reliance upon this information by third parties is prohibited and may be unlawful. Unless expressly stated, any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the National Research Fund. The recipient should check this email and any attachments for the presence of viruses. If you have received this email message in error, please delete it immediately and notify the National Research Fund through email.*

10.13 Staff Electronic Messaging Policy

10.13.1 Termination of Employment

When a staff member's employment with NRF ceases for any reason:

i. NRF shall deny the former staff member access to their electronic messaging account.
ii. The Head of Human Resources shall notify the DICT of such termination for the appropriate action.
iii. The staff clearance form shall give provision for DICT to clear such staff.

10.13.2 Withdrawal of Access

A staff's electronic messaging services shall be withdrawn, by the appropriate system administrator, when instructed by the Head DICT or their designate.

11.0 Appendix 9: End User Support Policy

11.1 Introduction

NRF has established various ICT services for staff and interns depending on each role in achieving the mandate, vision, and mission of NRF.

11.2 Purpose

This policy has been established to form the basis of support by DICT to the staff, interns and visitors who interact with NRF systems as they perform NRF's activities.

11.3 Scope

This policy covers the support provided to the staff, interns, and visitors using NRF-owned IT equipment. The support is limited for privately owned devices.

The policy shall support the provision of configuration, deployment and management of IT equipment owned by Divisions utilizing standardized operating systems, software configurations where appropriate and centrally licensed software packages.

11.4 General Policy Statements

11.4.1 Service limitations

i. DICT recommends using a supported Microsoft Windows operating system where possible as it can only provide limited support for Linux and Mac OS X operating systems.
ii. As privately owned IT equipment can have a vast range of unknown information in terms of compatibility and configuration, DICT is only able to provide limited support to devices not owned by NRF.

11.4.2 Restriction

i. The User Support service only provides support for NRF work and activities.
ii. DICT shall not provide support for operating systems no longer supported by their manufacturer (Windows XP for example).
iii. DICT shall not provide support for equipment which have passed its useable lifetime (usually 5 years).

11.4.3 DICT Responsibilities

i. DICT shall record all reported incidents and requests in the IT Service Management Tool to manage progress, keep the users up to date, fulfil requests and resolve incidents in line with our Service Level Agreements. This will also allow us to proactively improve the service based on frequently requested items and reported incidents.
ii. DICT shall advise users of the available services to be utilized to maximum effect.
iii. DICT shall manage relationships with suppliers in order to maintain continuity of service as appropriate.
iv. The service will be periodically reviewed to ensure that it is providing appropriate support for the business needs of NRF.

11.4.4 Customer Responsibilities

i. All service requests and incidents must be reported to the Service Desk immediately.
ii. Provide appropriate notice of equipment relocations.
iii. Provide the required information for IT to fulfill requests, resolve incidents, and promptly respond to requests for additional information.
iv. Provide service feedback and engage in service reviews with IT.

12.0 Appendix 10: Internet Usage Policy

12.1 Introduction

Internet connectivity presents NRF with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

i. Access to the Internet by personnel inconsistent with NRF needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet.
ii. Additionally, the company may face a loss of reputation and possible legal action through other types of misuse. All information found on the Internet should be considered suspect until confirmed by another reliable source.

12.2 Purpose

The purpose of this policy is to define the appropriate uses of the Internet by NRF employees and affiliates.

12.3 Scope

The Internet usage Policy applies to all Internet users (individuals working for NRF, including permanent full-time and part-time employees, contract workers, temporary workers, business partners, and vendors) who access the Internet through computing or networking resources. NRF's Internet users are expected to be familiar with and to comply with this policy and are also required to use their common sense and exercise their good judgment while using Internet services.

12.4 General Policy Statements

The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

- The Internet shall be used to increase staff access to information on matters related to the support of education and research.

i. Users of privately owned mobile systems shall obtain IP Addresses from the DICT Division upon filling a request form.
ii. All files downloaded from the Internet shall be scanned for malware using NRF anti-virus software with the latest virus detection updates.
iii. All Internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited.

12.5 Monitoring and Control

i. The DICT shall regularly inspect Internet files held on computers connected to NRF's network to ensure users have not accessed inappropriate sites or sites that have been expressly forbidden.
ii. Inappropriate sites will be filtered or blocked to ensure that users do not access their materials.
iii. Any user who finds a possible abuse, as well as security lapse on any system, report the event to the DICT.
iv. Users who deliberately access and/or inappropriate material or send inappropriate messages to others shall also have their Internet access withdrawn and shall be dealt with by NRF's disciplinary procedures.
v. NRF also reserves the right to report illegal activities to the appropriate authorities, *e.g.,* the Police.

12.6 Downloading

i. Information downloaded from the Internet shall be used for official purposes. Copyright laws shall be respected, and appropriate credit should be given to the author or source of the information.
ii. Any software or files downloaded via the Internet onto NRF's computers may be used only in ways consistent with their licenses or copyrights.
iii. No user may use NRF's facilities knowingly to download or distribute illegal software or material.
iv. No user may use NRF's Internet services to propagate any virus deliberately.
v. Users shall not use the Internet provided by NRF to access Internet-enabled activities such as gambling (betting) and excessive gaming.
vi. Acquisition, storage, and dissemination of data, which is illegal, pornographic, or negatively depicts race, sex or creed is expressly prohibited.
vii. Individual persons shall be held liable for any infringement of copyright laws due to downloaded information from the Internet or distribution of illegal software or material.

12.7 Peer-to-Peer (P2P)

i. Use of P2P applications (torrent) for file sharing and entertainment is deemed inappropriate and shall not be permitted.
ii. P2P usage enables sharing and distributing of copyrighted works, and the Copyright Act makes it illegal to make or distribute copyrighted materials without proper authorization from the copyright owner. Therefore, NRF shall enforce protocol or port-level restrictions to prevent P2P activities.
iii. Individual persons shall be held liable for any infringement of copyright laws due to sharing and distributing copyrighted works without proper authorization from the copyright owner.

12.8 E-Commerce

i. The use of NRF's Internet services to conduct business or e-commerce activities unrelated to NRF is expressly prohibited.
ii. The use of NRF's Internet services to hack other sites and, access unauthorized information within and outside NRF; stealing and using credit cards are criminal and prosecutable in the law courts.

12.9 Chat and Newsgroups

i. Users of chat Internet facilities like Facebook and Twitter shall identify themselves honestly, accurately and completely when participating in chats or newsgroups.
ii. Users may participate in newsgroups or chats during their work, but they do so as individuals, speaking only for themselves.
iii. Only those users who are duly authorized to speak to the media on behalf of NRF may write in the name of NRF to any newsgroup or Website.

12.10 Disclaimer of Liability for the Use of the Internet

i. NRF is not responsible for material viewed or downloaded by users from the Internet.
ii. Avoiding contact with inappropriate or offensive materials online is difficult. Users accessing the Internet do so at their own risk.
iii. Users must note that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are expected.

13.0 Appendix 11: Help Desk Triage Policy

13.1 Introduction

The primary role of DICT is to support end users in completing business tasks. In To ensure this role is carried out in a timely and high-quality manner, a policy has been established to help assign priority levels to problems or issues reported by end users to the ICT Directorate.

13.2 Purpose

This policy aims to establish service expectations and inform employees at NRF of the method by which help desk requests will be prioritized and what resolution can be expected of NRF ICT Policy.

13.3 Scope

This policy applies to all local and remote employees, management, contractors and other parties relying on access to NRF DICT and services.

13.4 General Guidelines

a. Before contacting the help desk, try the following:
    i) If data loss isn't a concern, reboot your system if possible.

ii) Find a resolution to the problem by reviewing available documentation, help sheets, and posted FAQs for the system presenting problems.
iii) Problems and requests designated as Level 1 Severity will take priority. Level 4 Severity issues hold the lowest priority.
iv) Problems and requests within a specific priority category will be handled on a first-come, first-served basis.
v) In some cases, special consideration will be given to mobile and remote employees whose access to Fund resources is more constrained.
vi) In the event of a natural disaster, failure of a third-party utility (such as electrical power), or some other catastrophic event, stated response and resolution times may be longer.

13.5 Priority Categories

The following table shows different priority levels for requests, a brief description of what constitutes each priority category, and timelines for problem response and resolution by the DICT.

Severity	Description	Response Time	Resolution Time
Level 1	• Critical system is down. • Functions not usable. • No workaround or alternative is available. • Data is corrupted. • Many end users are affected. • Regulatory/legal deadlines will be missed.	15 min	1 hour
Level 2	• Some functions are usable with severe restrictions. • No workaround or alternative is available. • Several end users are affected.	1 hour	4 hours
Level 3	• Basic functions are usable with minor restrictions. • Workaround or alternative is available. • One or more users affected.	4 hours	Next business day
Level 4	• Minor problem. • Functions are usable. • Defect is cosmetic or simply a nuisance.	Next business day	3 days

13.6 Contact Information

To report a problem or submit a request, use one of the mechanisms listed below. Kindly state your name, section/directorate/Division, e-mail address, telephone number, the

nature of the problem you are experiencing, the number of affected users, and the severity of the situation as it relates to your (or your colleagues') ability to complete necessary work.

i. Send an email.
ii. Fill out the job card / online form located on the intranet
iii. Call DICT main office

The following ICT Helpdesk procedures/guidelines are recommended:

i. Helpdesk receives the requests or inquiries from the end user through a phone call, request form, physical request, e-mail etc.
ii. Helpdesk officer records the request and assigns it a particular code/reference
iii. The help desk officer then informs the user/client of their code/reference assigned to the request forwarded for future reference and follow-up.
iv. Helpdesk then forwards the coded request to Administrator/Director DICT for scheduling to the respective section for action.
v. Administrator/Director DICT then forwards the coded request to the relevant section (Repair and Maintenance section, Systems Administration or to procurement or as deemed required) for action.
vi. The relevant section takes the necessary action, generating a report based on the action.
vii. The help desk updates the inventory of the requests through the administration management section.

14.0 Appendix 12: Backup Policy

14.1 Introduction

Data is one of NRF's most important assets. To protect this asset from loss or destruction, it must be safely and securely copied and stored.

14.2 Purpose

This policy governs how and when data residing on NRF's servers will be backed up and stored to provide restoration capability. The policy also outlines the procedures for restoring the backed-up data to individual systems.

14.3 Scope

i) This policy refers to the backing up of data on NRF's servers. Servers and the files and/or data types on these servers that are covered by this policy include:
   i. ERP server
   ii. Application server
   iii. Web and proxy server
   iv. Fund's Intranet
   v. E-Mail Server
   vi. Web Server
ii) This policy does not refer to backing up data on individual PC or notebook hard drives.
iii) Files that are left open at the time the backup procedure is initiated may not need to backed up.

iv) Before deploying a new server, a full backup must be performed and the ability to perform a complete restoration from that backup confirmed.
v) Before retiring a server, a full backup must be performed and placed in permanent storage.

14.4 Backup Schedule

NRF shall acquire a backup utility with features for both manual and automatic backup of selected files or resources.

a) Annual backups (permanent) are to be labelled using the following labeling Conventions: NRF-X, where X represents the year.
b) Backup drives stored on-site will be held in the ICT Designated Backup Safe.
c) Backup media stored off-site are to be stored in a designated off-site location known to the ICT Division's staff and managed by system administrators.
d) All backups will take place between the hours of 9 pm and 1 am.
e) Incremental backups (only files changed since the last backup) will be performed daily, Monday through Friday.
    i. These drives will be stored onsite during the following backup cycle.
    ii. At the end of the last cycle, the daily hot-swap disks will be removed to a predetermined offsite location for storage for 5 weeks.
    iii. When this 5-week period has elapsed, the hot-swap disk will be brought back on site for reuse for a period not exceeding one year.
f) A full backup will be performed each Friday.
    i. This Hot-Swap Disk will be stored on-site during the following backup cycle.
    ii. At the end of the last cycle, the weekly disk will be removed to a predetermined offsite location for storage for 5 weeks.
    iii. When this 5-week period has elapsed, the disk will be brought back on site for reuse for a period not exceeding one year.
g) A full backup will be performed at the end of each month. This disk will be immediately removed to a predetermined offsite location for permanent storage. These disks will never be reused.
h) All server backups performed must be noted in the server backup log immediately upon completion.
i) All server backup log sheets must be kept in an appropriately labelled three-ring binder in an agreed-upon, centralized location. The log must include the following:
    i. Date and time of backup,
    ii. Server name,
    iii. Name of administrator performing the backup,
    iv. Files backed up and/or skipped,
    v. Software used to perform the backup,
    vi. Backup medium used and its label/name,
    vii. Whether the backup was successful or not.
j) In the event the backup cannot be completed, is missed, or crashes, then it must be completed by 9:00 a.m. the following morning,

k) The reason for non-completion of the initially scheduled backup must be noted in the server backup log,
l) In addition, if a backup fails more than one day in a row, end users in NRF must be notified,
m) If a disk is discovered to be damaged or corrupt, then the disk must be destroyed to prevent further use and replaced with a new one.

14.5 Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential to regularly test one's ability to restore data from its storage media.
The following tests are recommended to be performed at the stipulated intervals:

a) All daily disks must be tested at least once every 3 months to ensure that the data they contain can be completely restored.
b) All weekly disks must be tested at least once every 3 months to ensure the data they contain can be completely restored.
c) All monthly disks must be tested at least once every 2 years to ensure that the data they contain can be completely restored.
d) Data will be restored from a backup if:
    - There is an intrusion or attack.
    - Files have been corrupted, deleted, or modified.

15.0 Appendix 13: Business Continuity Plan Policy

15.1 Introduction

Given the threats facing DICT and the institution, this policy provides a strategy to ensure critical systems are effectively recovered in agreed timeframes following a service disruption, outage or disaster.

15.2 Purpose

This policy is established to guide identifying and classifying an incident about its impact and assigning the appropriate level of control measures to recover the systems effectively and ensure the incidence doesn't recur.

15.3 Scope

The policy considers the restoration of ICT services within NRF and, as such, forms one part of a comprehensive Fund-wide business continuity plan (BCP)

15.4 Impact Assessment and Incident Management

15.4.1 Impact Levels

Information Systems Contingency Planning can be associated with the loss of any critical system or network, or part thereof, that may deny access to systems or significantly hinder the effective operations of NRF in providing administrative or external information services.

The impact of the loss can be graded as Extreme, Significant or Minor with the following broad definitions: (Note that the concept of escalation exists, in that an incident can be escalated from minor to significant and even to the point of extreme.)

15.4.2 Impact Description

Extreme -The most severe impact where the entire network is unavailable, or a large percentage of the organization has lost communications to central systems or central systems have failed, or there has been an incident that affects the organization as a whole (i.e., evacuation or data center fire) or the effect, whilst originally Significant, has been in play for such a period that it has been escalated too 'extreme'.

Significant -The effect on the NRF system is significant and affects multiple user groups or Divisions. For example, key NRF systems are impacted and/or important parts of the network are unavailable, or the effect, whilst originally minor, has been in play for such a period that it has been escalated too 'significant'.

Minor -The effect on NRF systems or network is minimal. A minor inconvenience to a specific group of users. Note that 'minor' incidents are, by definition, limited in their impact on a particular unit of operation rather than being Fund-wide. Therefore:

a) If a 'minor' inconvenience is felt in the organisation, then it will be considered significant; and
b) If a 'significant' incident is limited to a small group of users, it can sometimes be regarded as 'minor' at the NRF level.

15.4.3 Levels of Control

Not all incidents will require strategic or even tactical control; however, this depends entirely on the incident and the severity of the impact on the effective running of NRF. In the majority of ICT-related incidents, tactical control will suffice.

15.4.4 Impact Handling

a) Strategic control is often called 'Gold Command' in crisis management terminology.
b) Tactical control is often called 'Silver Command' in crisis management terminology.
c) In crisis management terminology, operational control is often called 'Bronze Command'.

Level	Description
Strategic	This refers to senior managers who make strategic decisions about the priorities of NRF. In an extreme incident, such as an evacuation of the campus, this team would control the communications channels and communicate strategic decisions directly to the tactical squad.
Tactical	A senior management team of subject matter experts within NRF. They are responsible for coordinating and directing the operational resources of NRF to ensure that the contingency plans are correctly executed.

Operational	The technical staff provides it with the detailed knowledge and capability to reconstitute systems and clearly understand what needs to be done and how.
Local	The management of incidents about systems that are 'local'.

15.4.5 Impact Handling Arrangements

Impact	Handling Arrangements
Extreme	Managed at a Strategic Control level, with the Strategic Control team relaying instructions and priorities to the appropriate staff.
Significant	Managed at the Tactical Control level with the Tactical Control team, relaying instructions to the appropriate staff, coordinating information, and reporting to the Strategic Control team as appropriate.
Minor	They are routinely handled by Operational Control staff.

15.5 Impact Management Procedures

15.5.1 Calling an Impact Assessment Level

Minor Incidents

i. Minor incidents shall be identified, addressed and logged routinely by operations staff and would not require the intervention of a tactical team. For example, the loss of a server or network router may require a routine reset of the machine, which may resolve the incident.

ii. In this case, the operations staff will make the call and resolve the incident, which would not be reported to higher levels of control.

In the case that an incident is not considered to be minor, either by its impact or due to what is estimated to be a prolonged recovery time, it will be escalated to a significant level or, in extreme circumstances, to a severe level.

Significant Incidents

i. A significant incident is called by the DICT staff responsible for managing the systems/network affected.

ii. This may be a direct call (due to the apparent severity of the incident) or because the operations staff has escalated the incident.

Extreme Incidents

i. The Director DICT calls an extreme incident. This may be a direct call (due to the apparent severity of the incident) or due to the incident being escalated by the operations or tactical management staff.

ii. In cases where the incident is considered so profound that it has a significant impact on the continuing operation of NRF, the Strategic Incident Management team will escalate the incident to the Executive Team, where it will be managed under the Business Continuity Planning process.

15.5.2 The Incident Management Process

The following table provides an overview of the approach to recovering from a disaster or incident.

Stage	Action	Details
Incident reported Declaration and impact assessment	Actions to be considered within this phase are contained within the contingency plans	• The plan is invoked immediately following the declaration of an incident
Stage 1 Emergency response	Damage assessment and resumption plan	• This phase may last a few minutes or hours following the incident-reported phase. • During this time, the disaster situation must be assessed and decisions made quickly regarding the course of action.
Stage 2 Recovery process	Continuity actions	• This phase may last several hours or several months following the Incident. • It ends when normal operations can restart. • Essential operations will restart and continue in recovery mode. • It will require actions from nominated personnel within NRF
Stage 3 Restoration of service	Restoration actions	• During this phase, conditions at Fund are restored to as near normal as practical. • Planning for this phase may start at the same time as the incident occurred. • However, if significant physical damage to infrastructure exists, this phase will not occur until much later.

Stage 4 Review	Review and service improvements	• Service risk log is reviewed and updated. • The incident is reviewed to identify any actions, changes or investments which can be made to reduce the risk of recurrence of the incident

15.6 Incident Management

The Strategic Management Team manages extreme impact incidents.

15.6.1 Strategic Management Team Responsibilities

The team shall carry out the following responsibilities:

i. Communication with key stakeholders;
ii. Decision to implement any resolution plans proposed by the tactical management team;
iii. Planning of and movement to the alternate site if appropriate;
iv. Approval of damage assessment and negotiation with insurers;
v. Media contact if required;
vi. Provision of management control and strategic direction;
vii. Approval of emergency equipment purchases;
viii. Securing financial and human resources as required;
ix. Approving all actions not pre-planned;
x. Resolving issues of priority to NRF;

16.0 Compliance

All users of NRF's ICT systems must read the ICT policy and declare that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the head of ICT.

Any user who breaches this policy shall face Fund disciplinary action.

16.1 Declaration Form

I have read and understood these Policy guidelines. I understand that violating the rules explained herein may lead to legal or disciplinary action being taken according to applicable laws, NRF regulations, statutes, code of conduct and/or policy.

Name: _____

Signature: _____

Date: _____

17.0 Policy Review

This policy will be regularly reviewed and amended as required to ensure it remains relevant and effective in meeting the Policy objectives. The responsibility for the ongoing review resides with the Head of ICT in conjunction with NRF ICT Committee. Any proposals during the intervening period should be submitted to the Head of ICT. Any changes to this policy shall be communicated to all users of NRF's ICT systems.

NACOSTI Building, 3rd Floor, Upper Kabete
P.O Box 26036-00100,
Nairobi, kenya
T: 254-20-4403386
E: info@nrf.go.ke
W: www.nrf.go.ke

National Research Fund Kenya