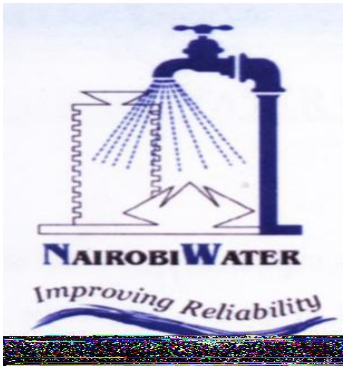
NAIROBI WATER & SEWERAGE COMPANY LTD.



INFORMATION COMMUNICATION & TECHNOLOGY POLICY

December, 2012

DOCUMENT CODE NCWSC/ICTD/ICT/02/MN/fo	Version 1.1
INFORMATION COMMUNICATION & TECHNOLOGY POLICIES	
FIRST REVIEW	

December, 2012

THIS DOCUMENT SHALL BE REVISED REGULARLY AS MAY BE NECESSARY

SIGNED: _____ DATE:_____

ICT DIRECTOR

PREFACE

The field of ICT has become more complex and dynamic, both in terms of technologies available and skills required. The Company has all along operated without an explicit ICT policy to guide its capacity utilization and address the emerging issues in this field. The Challenge for the Company is therefore to develop a clear vision and an appropriate implementation plan that will anticipate technological changes and identify ICT opportunities outside the traditional work practices. The development of this policy has therefore become a priority if the Company is to realize the benefits that ICT promises.

This Policy has made an effort in customizing public sector ICT guidelines and procedures and establishes structures that will integrate the use of ICT in the Company's operations for effective service delivery. The policy has also incorporated and amplified the aspirations of the country's Vision 2030 Strategy in ICT.

It is my belief that this policy, together with the accompanying ICT Strategy and structure will address the operational gaps that have existed and eventually transform the Company to a knowledge based institution of excellence in the water sector.

FOREWORD

The objective of the ICT Policy is to guide the mainstreaming of ICT in the Nairobi City Water and Sewerage Company Ltd (NCWSC). It has been developed in acknowledgement of the growing importance of ICT in supporting operations in the Company. The Policy aims at achieving efficiency and effectiveness accruing from the application of ICT, and ultimately improving service delivery. It is built on three pillars: Information Systems, Information Technology and Human Resources.

The concept of ICT starts with policies relevant to information systems that support all service areas, which are the basis for fulfilling the mandate of the Company. This policy provides guidelines on integrating the information systems within the Company for improved service delivery.

Information Technology is essential in ensuring that information systems operate as expected with the human resource acting as a catalytic ingredient that determines how systems perform and assist the Company in the discharge of its mandate. The people further develop, operate and manage information systems and information technology resources. Together these elements form the central theme of the ICT policy the Company has developed.

However, this policy goes beyond these elements in two important ways. First, it seeks to ensure that these essential elements are safeguarded and, secondly, that there is a recovery strategy in the event of failure. It is for this reason that the ICT Policy contains strong elements on security and business continuity policies.

The responsibility to ensure that the policy is effective lies with each of membership collectively. The NCWSC management on its part will play its role by ensuring each one of us is aware of its existence.

The Company is in the process of publishing the ICT Policy on its website, intranet and in hard copy, which shall be developed and updated annually by the ICT Directorate.

TABLE OF CONTENTS

PREFACE 3
FOREWORD 4
TABLE OF CONTENTS 5
ACRONYMS 7
DEFINITION OF TERMS 8
1.0 PART I - INTRODUCTION 11
1.1 Introduction 11
1.2 Background 11
1.3 Rationale 11
2.0 POLICY STATEMENT 12
3.0 AUTHORITY 12
4.0 VISION, MISSION AND OBJECTIVES OF THE ICT POLICY 12
4.1 Vision Statement 12
4.2 Mission Statement 12
4.3 Objectives of the NCWSC ICT Policy 12
5.0 SCOPE 12
6.0 KEY PRINCIPLES 13
7.0 ROLES AND RESPONSIBILITIES 13
8.0 PART II – INFORMATION SYSTEMS POLICIES 14
8.1 Information Systems 14
8.2 Data Management 15
8.3 Internet Based Systems 15
9.0 PART III – INFORMATION TECHNOLOGY POLICIES 16
9.1 Information Technology 16
9.2 Procurement 16
9.3 Inventory 17
9.4 Installation 17
9.5 Operations 17
9.6 Maintenance of ICT Equipment 17
9.7 Decommissioning of ICT Equipment 17
9.8 Disposal 17
10.0 PART IV – SYSTEM CONTROLS AND SECURITY POLICIES 18
10.1 Objectives 18
10.2 Systems Security Control Policy 18
10.3 Physical Security 18
10.4 Passwords 18
10.5 Data Security 18
10.6 Copyright and License Agreements 19
10.7 Internet 19
10.8 Email 19
11.0 PART V - BUSINESS CONTINUITY POLICIES 20
11.1 Responsibilities of the MD and Top Management 20
11.2 Risk Assessment 20
11.3 Business Impact Analysis 20
11.4 Recovery 20
12.0 MONITORING & EVALUATION 21
12.1 Compliance 21
12.2 Policy Review 21

ANNEX I: POLICY IMPLEMENTATION GUIDELINES 22
A. Guidelines for Information Systems 22
B. Guidelines on Operating Systems 22
C. Guidelines on Antivirus Software 22
D. Guidelines for Personal Computers and Servers 22
E. Guidelines for Procurement 23
F. Guidelines on Operations 23
G. Guidelines on Inventory of ICT Equipment 23
H. Guidelines for Decommissioning of ICT equipment 23
I. Human Resources and Development Guidelines 23
J. Guidelines on System Controls and Security 24
K. Guidelines on Email 26
L. Business Continuity 27
M. Risk Assessment 27
N. Business Impact Analysis (BIA) 27
ANNEX II: ACKNOWLEDGEMENT OF ICT SECURITY POLICY 30

ACRONYMS

BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Assessment
eCat	Electronic Catalogue
HR	Human Resource
ICT	Information Communication & Technology
MCA	Mission Critical Activities
PC	Personal Computer
NCWSC	Nairobi City Water and Sewerage Company

DEFINITION OF TERMS

ICT (Information and Communication Technologies)	ICT means technologies, including computers, telecommunication and audio-visual systems, that enable the collection, processing, transportation and delivery of information and communications services to users.
A Vision Statement	A **Vision statement** outlines what an organisation aims to be. It concentrates on future; it is a source of inspiration. An ICT Vision statement defines where the organization wishes to be in relation to application of ICT to its business.
ICT Mission	A **Mission statement** is a general statement of the overall purpose and aims of the ICT policy and strategies. It concentrates on present; it defines the customer(s), critical processes and the desired level of performance. It is a progressive roadmap towards the attainment of a vision.
ICT Policy	A **policy** is a deliberate plan of action to guide decisions and achieve rational outcome(s). Policy differs from rules or law. While law can compel or prohibit behaviours (e.g. a law requiring the payment of taxes on income) policy merely guides actions toward those that are most likely to achieve a desired outcome.
ICT System	An ICT system definition includes, but is not limited to, hardware, software and communications equipment that the Company uses to communicate, process and store information. The organization and structures involved in relating all these systems, the information they store and the people involved in the administration and maintenance.
User	A user means any person who is recognized by the Company as having a valid reason to access the Company ICT systems whether that access is from within the Company or outside the Company
Alternate Site	Alternate Site means a site held in readiness for use in the event of a major disruption that maintains an organisations' business continuity.
Business Continuity	It is a state of continued, uninterrupted operation of a business.
Business Continuity Management:	It is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely fashion in the event of disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.
Business Continuity Plan:	This means a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organisation in the event of a disruption.

Business Impact Analysis	**This** means the process of identifying, and measuring (quantitatively and qualitatively) the business impact loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements and essential staff and to help shape the business continuity plan. All impacts should be measured on financial, regulatory, legal and reputational damage basis.
Communication Protocols	This means an established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.
Critical Services	It means any activity, function, process or service, the loss of which would be material to the continued operation of a financial institution.
Crisis	It is an event, occurrence and/or perception that threaten the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an institution.
Crisis Management Team:	It means a team consisting of key executives, key role players (i.e. legal counsel, facilities manager, disaster recovery coordinator), and the appropriate business owners of critical functions who are responsible for recovery operations during a crisis. Evaluation of capability, training, testing of Crisis Management teams maturity level must be documented.
Disaster	This is a sudden, unplanned catastrophic event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time, causing unacceptable damage or loss.
Emergency Response Team	It's any organization that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals)
Exercising	This is the process through which business continuity plans are tested and rehearsed in a controlled environment using team members and staff.
Major Operational Disruption	It is a high impact disruption of normal business operations, affecting a large geographic area and adjacent communities that are economically integrated to it.
Operational Risk	It means the risk of loss from inadequate or failed internal processes, people and systems or from external events.
Recovery	This is the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.

Resilience	Means the ability of an organisation, network, activity, process or financial system to absorb the impact of a major operational disruption and continues to maintain critical operations or services.
Risk Assessment	It means the probability and impact of specific threats being realised.
Single Point of Failure	It is a unique source of a service, activity, and/or process where, there is no alternative and whose loss could lead to the failure of a critical function.
Administrators	Person responsible for management of a particular aspect of ICT resources
Manager/ Supervisor	Person overseeing overall ICT resources in managing access rights and work allocation.
User	Any person authorised by way of access rights to use an ICT resource.
Portal	An organisation's data/information resource accessed via internet for public usage.

1.0 PART I - INTRODUCTION

1.1 Introduction

The technical committee of the Board provides regular, timely and accurate advice and direction on policy formulation, planning and implementation. The Committee will review the effectiveness of NCWSC's ICT technologies, their effectiveness and relevance to the functions in service delivery to its customers.

The technical committee is mandated to oversee the implementation of the automation of NCWSC processes. Its functions also include but not limited to:

- Evaluating the overall effectiveness of ICT technologies developed and implemented
- Reviewing compliance matters that may have a material impact on the company's ICT policies.
- Developing strategies and policies for ICT systems.
- Developing an ICT policy for NCWSC
- Receiving and reviewing the ICT proposals for ICT implementation.
- Reviewing all contracts, agreements or other instruments involving the ICT affairs.
- Assuming such other responsibilities as from time to time may be delegated by the Board.

Additionally, the committee provides technical advice in regards to the implementation of the all ICT related systems. In instances where the Company is required to procure and install ICT equipment and software, the Committee provides technical advice in terms of technical specifications and subsequent evaluation of tenders.

1.2 Background

In 2006, the Company adopted a five-year Strategic Plan (2006-2011) that outlined its overall vision, mission as well as other ways to improve delivery of services. One of the areas that the Company is giving considerable attention is the formulation and implementation of an ICT policy and strategy.

The Company is aware that most institutions in both the public and private sectors are re defining their policies and strategies to embrace ICT. The immediate challenge for Company is to establish short, medium and long-term ICT plan and adoption of an enabling policy. There is also need to harmonize and integrate existing systems, present and future initiatives. In this regard efforts to establish appropriate ICT standards, data security systems and procedures as well as related quality assurance mechanisms are a priority.

1.3 Rationale

ICT capacity in NCWSC has grown as demonstrated by the number of equipment and the personnel who have received basic, functional and specialized training. ICT infrastructure has also been improved by the installation of Local Area Network at the company headquarters and its regional offices within and outside Nairobi.

The current challenges being experienced by ICT services are occasioned by the level of existing capacity in terms of technology, lack of information systems integration, state of facilities and infrastructure. The service objective is to increase the capacity of NCWSC staff to access data and process information necessary for improved service delivery. It is also envisaged that operations at NCWSC will be automated and interconnectivity between NCWSC and all other outer stations will be achieved.

2.0 POLICY STATEMENT

The Company will continuously enhance its organizational capacity by adopting modern technology and skills development. This policy will ensure that ICT resources are optimally utilized in order to achieve efficiency in service delivery. It will facilitate efficient and effective service delivery through timely provision of a robust ICT infrastructure, application software, support services and operational capacity.

3.0 AUTHORITY

The policy derives its authority from;

(i) NCWSC Strategy Paper (2006-2011)
(ii) NCWSC Procurement Manual

4.0 VISION, MISSION AND OBJECTIVES OF THE ICT POLICY

4.1 Vision Statement

"To be a knowledge based institution of excellence in the water sector".

4.2 Mission Statement

"To mainstream the use of ICT in the Company's operations for improved service delivery to its customers".

4.3 Objectives of the NCWSC ICT Policy

The objectives of NCWSC's ICT policy are to:

(i) Support the development and implementation of ICT in the Company
(ii) Ensure development and maintenance of ICT systems
(iii) Promote efficient and effective operations and usage of ICT systems within the Company
(iv) Facilitate the development of ICT skills to support ICT systems in the Company
(v) Encourage innovations in technology development, use of technology and general work flows within the Company
(vi) Promote Information sharing, transparency and accountability within the Company and towards the general public
(vii) Promote efficient communication among the Company's staff, customers and/or stakeholders
(viii) Ensure that ICT facilities are fully accessible to all staff

5.0 SCOPE

The ICT Policy shall apply to all the Company's employees and stakeholders. The policy will address Information Systems, Information Technology, Human Resource Development, Governance and Business Continuity strategies in relation to the Company's operations.

6.0 KEY PRINCIPLES

This policy shall be guided by the following key principles:

(i) Mainstreaming of ICT in the Company
(ii) Seamless integration of ICT platforms
(iii) Inclusion, flexibility and support of other quality management systems
(iv) Adherence to best practices & policies
(v) Economies of scale and customer value propositions

7.0 ROLES AND RESPONSIBILITIES

The overall responsibility of implementing this policy will lie with the Corporate Technical Committee which will be responsible for the overall strategic management of ICT resources in the Company. The Committee will draw representation from NCWSC Board members and co-opt other members from the staff of NCWSC who in their opinion will add value to the work of the Technical Committee.

Specifically, the Committee will be responsible for oversight, enforcement and review of the policy and the initiation of ICT projects.

8.0 PART II – INFORMATION SYSTEMS POLICIES

8.1 Information Systems

Information Systems policies are intended to support structured approach to acquisition, development, operations and maintenance of information systems in the Company. In this way, the Company will guarantee their success and, therefore better decision support to meet its mandate. The ICT Directorate is the sole custodian and technical administrator of all Information Systems and Applications in the Company.

8.1.1 Application Systems

8.1.1.1 Initiation of a Software Project

All software acquired and developed shall be used strictly for NCWSC purposes only. Every software acquisition or development request shall be initiated through a written statement of scope and objective. The written statement will be submitted to the Company's Technical Committee.

8.1.1.2 Acquisition

With respect to software acquisition:

(a) The Company will use packaged software as the preferred option
(b) In the event that custom development of software is proposed, the request for such development must be justified on case by case basis
(c) Only open source software with technical support shall be used with approval of the ICTD

8.1.1.3 Development

With respect to software application development:

(a) Each software development project will be initiated on the basis of an approved requirements specification which:
   - Identifies user requirements (functional requirements) expressed in non-technical language
   - Provide return on investment analysis
   - Identifies beneficiaries
(b) If the Requirements (specifications) are approved the project sponsor and owner will proceed with the technical Specification to express user requirements specified in technical language
(c) The NCWSC shall purchase only fully licensed copies of computer software
(d) User testing and acceptance are the necessary and sufficient conditions for systems commissioning

8.1.1.4 Maintenance

Application software maintenance is critical for effectiveness and efficiency of the system. The following policy will therefore apply:

(a) Access to live systems will be restricted to authorized users
(b) Application software purchased must have service level maintenance agreements to ensure continuity
(c) Only certified or supplier authorized agents will be allowed to provide maintenance
(d) Internal maintenance shall be provided by personnel trained and certified
(e) Maintenance contracts for Information systems in the Company shall be managed by ICTD

8.1.2 Operating Systems

The following policies are intended to facilitate the governance of office automation within the Company:

(i) Microsoft's Windows Operating Systems will be the preferred Operating System for all computers
(ii) The Company will standardise its office productivity tools on the Microsoft Office suite
(iii) Commonly used functions that require the same templates will be supported through issuance of Company-specific templates

8.1.3 Anti-virus Software

With respect to anti-virus software:

(i) The ICT Director shall ensure availability and continuous update of anti-virus protection on all computers, laptops and servers
(ii) No person shall be allowed to connect private PCs, laptops, modems or any ICT peripheral to Company's network or hardware
(iii) All removable media in use within the Company must be scanned for viruses.

8.2 Data Management

In order to ensure that data and information are available as and when required, the following policies will be adopted:

(i) It is the responsibility of heads of functional areas in close consultation with the ICT Director to determine and design the data that should be available in the Company
(ii) The ICT Director will ensure overall data capture, availability, accuracy, confidentiality, and integrity.
(iii) The Company will acquire systems and tools to create, process, manage and preserve data
(iv) The data shall be classified into Confidential and Public

8.3 Internet Based Systems

The ICT Director will adopt and develop the following internet based systems as a means of communication and service delivery:

(i) Websites
(ii) E-mail systems
(iii) Short Message services
(iv) Intranet
(v) Collaborative systems

9.0 PART III – INFORMATION TECHNOLOGY POLICIES

9.1 Information Technology

The objectives of Information Technology policies must be consistent with public sector standards issued by relevant authority such as the NCWSC procurement Manual and E-Government Secretariat, Legal authorities, National Single Window System.

9.1.1 Desktop Computers

(i) The Company shall seek to:
  (a) Standardize hardware equipment to minimize multi brands
  (b) Allocate computers to user departments appropriately
  (c) Provide uninterrupted power supply and protection to all ICT installations in order to protect the systems from power fluctuations and surges
  (d) Review hardware specifications to be in line with current technological trends

(ii) Users are accountable for all ICT equipment allocated to them

9.1.2 Laptops

With respect to laptops:

(i) Laptops will be procured for service areas and assigned to officers whose nature of work merits their use
(ii) Hardware specifications will be reviewed to be in line with current technological trends
(iii) Users are accountable for all laptops issued to them
(iv) There will be no additional software installation without prior authority from the ICT Director

9.1.3 Servers

The following best practices will be adhered to with respect to server deployments within the Company:

(i) Maximization of the storage system
(ii) Ensuring online and offsite backups and real-time replication for critical applications
(iii) Disaster prevention arrangements (see Business Continuity)
(iv) The acquisition of servers should be standardised to avoid multi brands
(v) All servers other than for backing up and disaster recovery shall be located in a central server room
(vi) The ICT Director will be responsible for the administration of all the servers in the NCWSC
(vii) Provide uninterrupted power supply and protection for all servers
(viii) Review hardware specifications to be in line with current.

9.2 Procurement

The procurement of hardware, software, peripherals and network products shall be guided by NCWSC procurement rules and regulations and:

(i) Must conform to minimum specifications and standards established by the ICT Director
(ii) Must be informed by annual procurement plans
(iii) Take into account software requirements and anticipate future requirements
(iv) The MD will approve directly procurement of ICT emergency equipment, be it from manufacturers, authorised dealers and/or certified service centres
(v) Must have warranty

9.3 Inventory

(i) The Company shall establish and maintain an inventory of all ICT equipment in the service areas.
(ii) In the event of movement of officers occasioned by deployment or exit, the head of the affected service area shall reallocate any ICT equipment under their custody and communicate the same to the ICT Director for purposes of updating the inventory
(iii) Movement of ICT hardware from one office to another is restricted

9.4 Installation

On installation of information technology products:

(i) An Installation Certificate must be issued and signed by the head of ICT who shall be involved in the entire installation process
(ii) The head of the service area shall be responsible for all installations
(iii) All installations must be in accordance with the supplier standards and Association's requirements

9.5 Operations

(i) All operations must have User and Technical manuals from the supplier
(ii) The operating environment must conform to the minimum manufacturers' specifications or international standards
(iii) Emergency procedures must be clearly displayed in the server room and data centre

9.6 Maintenance of ICT Equipment

Maintenance of ICT equipment is critical for effectiveness and efficiency of NCWSC operations. The following policy will therefore apply:

(i) ICT hardware purchased must have Service Level Maintenance Agreements on expiry of the warranty;
(ii) Only certified manufacturer authorized agents will be allowed to provide maintenance
(iii) Internal maintenance shall be provided by personnel trained and certified
(iv) Maintenance contracts for ICT equipment shall be managed by the ICT Director

9.7 Decommissioning of ICT Equipment

With respect to decommissioning ICT equipment:

(i) All ICT equipment shall have a predetermined life span
(ii) There must be written justification by the head of ICT for decommissioning of any ICT equipment
(iii) Equipment that are no longer effective or in use will be decommissioned within 6 months after the review
(iv) ICT equipment will be decommissioned after an installation certificate has been issued for replaced systems
(v) A Decommission Certificate will be issued on successful conclusion of the exercise

9.8 Disposal

Information technology resources disposal must:

(i) Be in accordance with the existing public disposal rules and regulations
(ii) Avoid or minimize degradation to the environment
(iii) Seek to re-use some of or all the computer components
(iv) Seek authority to donate any retired computer equipment
(v) Remove data and systems on all hardware to be disposed off
(vi) Comply with manufacturer, supplier or service provider terms and conditions of disposal
(vii) Be indicated on the Disposal Certificate

10.0 PART IV – SYSTEM CONTROLS AND SECURITY POLICIES

The Company has invested substantially in ICT resources. These resources are vital in realizing the Company's business objectives and are integral to the ability of the Company to operate effectively. This policy establishes general guidelines, rules and regulations for the use and protection of the Company's information and ICT systems. The implementation of this policy will thus promote the availability, integrity and confidentiality of the Company's ICT systems.

10.1 Objectives

(i) Create general awareness on appropriate security measures that must be implemented to safeguard the effective operation of the Company
(ii) Highlight the responsibilities necessary for the protection of ICT systems
(iii) Facilitate the preservation of the integrity and privacy (confidentiality) of the Company's information
(iv) Protect and promote the Company's reputation

10.2 Systems Security Control Policy

The Company's ICT systems, and the service they provide, will be protected by effective control of security risks at all levels of the organisation, providing, managing and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved

(i) **Access:** Access to the systems will be restricted to authorized users as determined by the head of a service area
(ii) **Breaches:** Any breach of this policy shall be dealt with under the Company's Disciplinary Policy and Procedures. In addition, the Company may advise law enforcement agencies of the breach where it considers that a criminal offence may have been committed
(iii) **Review:** The Technical Committee will establish a sub-Committee whose responsibilities will include the review of this aspect of the ICT policy at intervals of six months and amended as need arises. Any changes shall be communicated to all users of the Company's ICT systems.

10.3 Physical Security

ICT resources are generally exposed to the risk of unauthorized access, manipulation, disruption and natural disasters. In an effort to protect the ICT equipment and systems and ensure their availability the Company will institute appropriate control measures to ensure that its ICT resources are safeguarded. Appropriate controls will be established to limit access to ICT infrastructure, computer equipment and data, commensurate with the acceptable level of risk. The access to the Company's ICT systems shall be reviewed every six (6) months.

10.4 Passwords

The ICT department shall prevent unauthorized access to the Company's corporate computer systems. Such controls shall take the form of passwords in the user identification process.

10.5 Data Security

The head of ICT shall develop rules, regulations and guidelines that ensure confidentiality, integrity, availability and safety of all Company information.

10.6 Copyright and License Agreements

Only licensed software shall be used in the Company. Copying and distribution should not be done without the necessary licenses. The ICT directorate will ensure that all software applications used by the Company complies with the relevant licensing agreements, compile all relevant licensing agreements and maintain a record.

10.7 Internet

(i) To ensure productive, appropriate use and to minimize risks, access to the Internet should be limited to staff who need it for their work. Users should use the Internet in an effective, ethical and in a lawful manner.

(ii) Users should not use the Company's Internet access to view, print, distribute, display, send or receive images, text or graphics of offensive or obscene material or material that violates any Kenyan law.

(iii) The Company shall maintain a log of sites visited as a means of determining appropriate usage.

(iv) The Company shall install and maintain firewalls to filter content coming in or going out via the internet and protecting external attacks.

10.8 Email

(i) The Company encourages the use of email and respects the privacy of users. The Company will not routinely inspect, monitor or disclose the contents of email without the consent of the user. However, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the Company may inspect, monitor, or disclose email when the Company believes that it has a business need to do so. The use of email must be related to the Company's business activities.

(ii) For proper utilization of server disk space, uncollected mails will be disposed after every forty five (45) days. Mail users will be allocated disk quotas for storing mail. Use of email is permitted as long as it does not:

- (a) Violate this policy
- (b) Degrade the performance of the network
- (c) Divert attention from work

(iii) A disclaimer shall be applied to all outgoing email (See Annex I)

11.0 PART V - BUSINESS CONTINUITY POLICIES

Major operational disruptions pose a substantial risk to the continued operation of the Company. The extent to which the Company incorporates the risk of a major operational disruption in its business continuity plan is dependent upon its risk profile.

(i) The Company shall ensure the implementation of the business continuity plan by periodically conducting a business impact analysis at least once a year.

(ii) An organizational risk assessment, risk management and risk monitoring to identify the mission critical activities and potential for major disruptions will also be undertaken. The Company should also provide sufficient human and financial resources to support Business Continuity Management.

11.1 Responsibilities of the MD and Top Management

The responsibility for business continuity management rests with the Company and the senior management who are expected to formulate business continuity policy reviews, procedures and guidelines. All these must be documented and reviewed after every two (2) years. MD and senior management shall be responsible for:-

(i) Institutionalising Business Continuity Management Document

(ii) Defining the roles, responsibilities and authority to act in the event of a major disruption

(iii) Constituting Business Continuity Management Team consisting of:

- (a) MD
- (b) Coordinator (drawn from the technical Committee)
- (c) Department Heads
- (d) ICT Director

(iv) Constituting Crisis Management Team consisting of all heads of critical operational areas

(v) Accountability for business continuity management in cases of outsourced business continuity function.

11.2 Risk Assessment

A risk assessment examines the most urgent business functions identified during business impact analysis. It looks at the probability and impact of a variety of specific threats that could cause a business disruption. The Company shall undertake a Risk Assessment of its ICT processes every one (1) year.

11.3 Business Impact Analysis

Business impact analysis forms the foundation upon which the business continuity plan is developed. It identifies critical business functions and operations that need to be recovered on a priority basis and establishes appropriate recovery objectives for those operations. It should be completed in advance of a risk assessment in order to identify the urgent functions upon which a risk assessment should be focused.

11.4 Recovery

(i) The Company shall develop recovery procedures that reflect the risk they represent to the operation of its systems taking into consideration the interdependency of risks

(ii) The Company shall facilitate testing of plans to ensure that crisis and recovery teams are aware of their roles and responsibilities in the event of a disruption

(iii) In cases where the Company shares or outsources a disaster recovery site, there must be service level agreements or contract in place that clearly outline the terms that govern these arrangements between the parties

(iv) Recovery solutions must be based on Business Impact Assessment (BIA) information

12.0 MONITORING & EVALUATION

All ICT systems, as with all other assets, are the property of the Company. The Company therefore reserves the right to monitor these systems to ensure compliance with this policy. The monitoring of the ICT system activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

(i) Users of the Company's ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the Company's ICT resources should avoid storing information on these systems that they consider private. By using the Company's ICT systems, users expressly consent to the monitoring of all their activities within the Company's ICT systems.

(ii) During the implementation of this policy, the Company will ensure that there is continuous monitoring and evaluation for efficiency, accountability and transparency. The Monitoring and Evaluation will be carried out by the ICT internal team in consultation with the corporate Technical Committee.

12.1 Compliance

All users of the Company's ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the head of ICT. A sample declaration is provided in Annex II.

12.2 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 on-going review resides with the head of ICT in conjunction with the Company ICT Committee. Any proposals during intervening period should be submitted to the Head of ICT. Any changes to this policy shall be communicated to all users of the Company's ICT systems.

ANNEX I: POLICY IMPLEMENTATION GUIDELINES

A. Guidelines for Information Systems

1. Application Systems

(i) The selection of a supplier or system developer should be carried out in accordance with the existing rules and regulations on public procurement.

(ii) The duplication of copyrighted software or documentation is strictly prohibited unless for backup purposes.

2. Installation/Operation

The installation and operation of systems will involve the following: -

(i) Preparation of end users with awareness and training prior to deployment. [This is to ensure best results and to avoid unnecessary calls to user support].

(ii) Maintenance of full documentation with respect to configurations, changes, and other "as installed" parameters. This will facilitate efficiency in management of operations, especially in the event of staff changes].

(iii) Software will be installed in accordance with licence agreements. Software will be installed and rolled out only after issuance of an acceptance testing certificate.

(iv) Systems shall be commissioned only after being tested and accepted.

B. Guidelines on Operating Systems

(i) Software drivers to support efficient use of the Microsoft Office suite will be accessible centrally from a designated server;

(ii) Updates of the Office Productivity software will be carried out as and when new versions are released.

C. Guidelines on Antivirus Software

(i) Any new computer or laptop shall be installed with the most current antivirus software

(ii) Any virus-infected computer must be removed from the system until it is certified as being virus free.

D. Guidelines for Personal Computers and Servers

(i) Users are required to lodge a report of any malfunction of the computer they use on the prescribed problem reporting system or mechanism to the head of ICT.

(ii) Laptops should not be carried out of NCWSC building except for Company's work outside the building. All laptops to be carried outside for external use must be logged.

(iii) Hardware specifications should be reviewed biannually by the head of ICT.

(iv) The operating environment for all data centres and server rooms should be consistent with the manufacturers' specifications.

(v) Server storage should be structured logically and space allocation quotas enforced.

E. Guidelines for Procurement

(i) The head of ICT shall undertake an annual survey to determine needs and impact of ICT resources in the Company
(ii) Requests by any service area for the procurement of ICT related goods and services shall be validated by head of ICT
(iii) Technical evaluation and inspection of ICT equipment shall be done under the supervision of the Head of ICT strictly on the basis of the technical specifications
(iv) Deployment of procured ICT equipment shall be done by the Head of ICT, strictly on the basis of identified and validated needs

F. Guidelines on Operations

Guidelines covered under physical Security sub section shall apply

G. Guidelines on Inventory of ICT Equipment

(i) Inventory must include serial number, date of issue, location/service area, model, type, head of service area, responsible officer and functional condition
(ii) Inventory of computers should be reviewed and updated continuously
(iii) The head of ICT shall conduct an annual inventory check of all ICT equipment
(iv) In the event of any movement of ICT equipment from one office to another, the same should be communicated to the head of ICT for purposes of updating the inventory

H. Guidelines for Decommissioning of ICT equipment

(i) At the end of five (5) years after the procurement of the equipment, a review shall be done for the purpose of determining its continued usage, or discontinuity
(ii) For equipment that have been in existence for five (5) years and above, a comprehensive review shall be carried out immediately the policy is effective
(iii) For all newly acquired equipment, a post installation review shall be carried out 6 months after commissioning while subsequent reviews will be undertaken every two(2) years
(iv) All the data and software must be removed before decommissioning

I. Human Resources and Development Guidelines

The Company will upgrade ICT skills and knowledge of all its employees and agents annually. This will include: -

(1) End User Training

It is a requirement that all newly recruited NCWSC employees must possess basic computer skills. End user training programme will include the following content: -

(i) Refresher course on basic computer user skills and specialized system run by NCWSC
(ii) Overview of ICT policies and guidelines
(iii) Skills specific to particular applications
(iv) Security and best practices

(2) Technical Training

Technical training programme will include the following content: -

(i) Support related training (depending on area of assignment and deployment);
(ii) Professional Certification (in the area of specialization);
(iii) Overview of ICT policies and guidelines
(iv) Security and best practices
(v) Advanced Data Communication and networks

(3) Membership/Management Training

This level of training programme shall include the following content: -

(i) Basic System usage skills
(ii) Overview of ICT policies and guidelines
(iii) Skills specific to particular applications/systems
(iv) Security and best practices
(v) Use of management reporting tools

J. Guidelines on System Controls and Security

All users of the Company's ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the head of ICT. A sample declaration is provided in the Annex II.

Responsibilities

(i) The ICT Director has overall responsibility for security management policy.
The officer shall:

(a) Ensure the compliance, establishment and implementation of the ICT security policy
(b) Provide support and guidance to assist users in understanding their responsibilities with regard to ICT security
(c) Ensure that all users are aware of this policy and are in compliance with it
(d) Maintain appropriate controls to ensure adherence to this policy
(e) Ensure that breaches of security are dealt with in a coordinated and timely manner and reported to the head of ICT
(f) Ensure compliance with the Company's ICT security policy
(g) Gauge the effectiveness of the ICT security measures through regular monitoring programs
(h) Report to the Technical Committee on the irregularities and any breaches of ICT security policy

(ii) User Responsibilities
The Users of the Company's information systems are accountable and responsible for

(a) Understanding and adhering to this policy
(b) Notifying any breach of ICT security to the head of ICT or immediate supervisor

(iii) Systems Access
Access to ICT equipment and systems shall be restricted to authorized users through the use of logon identities, passwords, locks and access control devices. The use of system logon identities shall be unique to each authorized user. All logon identities shall be authorized by at least two managers of the respective system.

(iv) Physical Security
The creation of user identities shall be as follows: -

(a) Access to secure areas of the Company shall be authorized by the Information systems security manager in consultation with the head of ICT
(b) Access to the Company's ICT network shall be authorized by the head of ICT
(c) Access to the Company's business applications shall be authorized by the appropriate Officer

(v) Physical Security Rules
The following rules relate to physical security:

(a) The company secure areas, must be physically strong and protected against weather elements and hazards including rain, floods, fire, extreme temperatures, tremors, dust and lightning

(b) Entry into secure areas will be restricted to unauthorized users
(c) Visitors to secure areas shall be permitted only under strict supervision of an authorized ICT staff and a log shall be kept for each visit
(d) Secure areas shall be protected against intrusion by use of appropriate surveillance systems or by security personnel
(e) Combustible material shall not be kept near ICT equipment
(f) Air temperature and humidity must be controlled within acceptable limits
(g) All computer devices must be adequately protected against interruptions to electricity supply
(h) Computing equipment must not be removed from the Company's premises unless written approval is given by the head of ICT or any other relevant authority

(vi) The ICT Director must ensure that:
(a) Access to the server rooms is restricted to unauthorized users and that access is by an access control device
(b) All ICT equipment leaving the NCWSC premises are accompanied by a valid authorisation by way of a gate pass
(c) There is consistency between the serial numbers on the equipment and the gate pass
(d) All non NCWSC ICT equipment coming into the company premises must be declared and registered

(vii) Responsibility of users:
Users must:
(a) Not remove any computer device from the Company's premises without written
(b) Take Responsibility selecting appropriate password and securing their password
(c) Ensure that their passwords are periodically changed. It is essential that access to ICT systems should be through the use of strong passwords
(d) Ensure that their passwords are periodically changed. It is essential that access to ICT systems should be through the use of strong passwords

The following rules govern the use of passwords:
(e) All passwords must be changed on at most a quarterly basis
(f) Passwords will consist of a minimum of 6 alphanumeric characters
(g) Passwords will be kept private i.e., not shared, or written down
(h) Logon IDs and passwords should be suspended after a specified period of disuse
(i) Logon IDs and passwords should be suspended after a set number of unsuccessful log on attempts
(j) Passwords should not be repeated or be similar to previous passwords, application systems will be set to remember the last 5 passwords;
(k) Passwords should not be the word "password" or a similar word in English or vernacular
(l) Passwords should not be a common usage word such as:
- Names of family, pets, friends, co-workers etc ;
- Computer terms and names;
- The words NCWSC or any derivation;
- Birthdays and other personal information such as addresses and phone numbers;
- A word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

(viii) Data Security

(a) In the event of confidential information being lost, either through loss of a computing device or other breach in security, the ICT Director should be notified immediately. No attempts should be made to recover data without authority from ICT Director.

(b) Personal data such as music, video, images, documents should not save on the network server.

(ix) Responsibilities of ICT Director

The Head of ICT must ensure that:

(a) A backup policy and procedure that covers all Company data is developed

(b) The necessary storage space for users to store Company information is provided

(c) Backups of Company data are stored in an access-controlled area

(d) Database integrity is achieved

(x) Responsibilities of Users

Users must ensure that:

(a) All Company data and files are saved on a network server for which they have been assigned as opposed to the local hard disc

(b) Portable computer storage devices must be stored securely when they are not being used

(c) Portable computer storage devices that are to be disposed must be done securely

(d) All software used on the Company's ICT system must be licensed

(e) Computer Viruses: The following rules govern the use of the anti-virus application:

- All virus definitions must be currently updated and should not be more than two weeks old
- Any PC on the network should be scanning for viruses automatically as it boots

K. Guidelines on Email

(i) The following disclaimer will be applied to all outgoing email:

"This email is confidential and intended for the sole use of the individual or entity to which it was addressed. If you have received this email in error please notify the sender immediately and delete this email without disclosing, copying, using, distributing or storing its contents. Kindly note that 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 Company. The recipient should check this email and any attachments for the presence of viruses. The Company accepts no liability for any damage caused by this email."

(ii) Email must not be used to:

(a) Reveal or publicize confidential or proprietary Company information

(b) Send or forward emails containing defamatory, ethnic, offensive racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor

(c) Send copies of documents in violation of copyright laws

(d) Harass, intimidate or interfere with the ability of others to conduct the Company's business

(e) "Spoof" i.e. sending an email so as it appears to be from someone else

(f) "Snoop" i.e. obtaining access to the email of other people for the purpose of satisfying ones morbid curiosity

(g) Attempt to breach any security measures on the email system

(h) Attempt to intercept any email transmission without proper authority

(i) Send "Spam" i.e. unsolicited email message

(j) Propagate viruses or generate high volume of network traffic that degrades the performance of the network

(k) Send confidential emails without the use of suitable encryption

L. Business Continuity

(i) Office, data centre or server room recovery must not be in the same building or close to the normal business operation

(ii) Documented pre- and post- test reports are to be completed for all recovery testing.

M. Risk Assessment

(i) The BC Management Team shall report on the status of business continuity management to the Company and senior management on a regular basis, highlighting where there are identified gaps. This is through implementation status reports, incident reports, testing results and related plans for strengthening the business continuity plan.

(ii) A risk assessment is at a minimum expected to achieve the following;

(a) Identify unacceptable concentrations of risk and what are known as 'single points of failure.

(b) Identify internal and external threats that could cause a disruption and assess their probability and impact

(c) Prioritize threats within the institution

(d) Provide information for a risk control management strategy and an action plan for risks to be addressed

(e) Mitigation of risks through a documented remedial plan.

(iii) Methods and Techniques

The methods and techniques to be used to provide risk assessment include

(a) Insurance statistics

(b) Published disaster frequency statistics

(c) Scoring systems for impact and probability

(d) Gap analysis

(e) Stress testing

N. Business Impact Analysis (BIA)

At a minimum a business impact analysis is expected to

(i) Provide an understanding of NCWSC's most critical objectives, the priority, and the timeframes for resumption of each

(ii) Provide information about resource requirements over time to enable each business function within the organization achieve continuity or resumption of activity within the established timeframes. It should at a minimum identify

(a) Staff numbers and key skills

(b) Data applications and systems

(c) Facilities including alternative location needs, backup strategy policy and schedule. Vendors/suppliers of various services

(d) Constraints

(e) Mission Critical Activities (MCA's) or tasks that need to be recorded to ensure continuity of the process and business

(f) Dependencies on people, systems, processes, internal and external parties

(g) Systems impact assessment highlighting

(h) Location

(i) Department unit owners, system information, commissioning Dates

(j) Technical person responsible

(k) Provide a list of recovery options for each business process

(iii) Methods and Techniques
A combination of the following tools and techniques may be used to carry out Business Impact Analysis:
(a) Questionnaires
(b) Interviews
(c) Workshops

(iv) Generally a combination of all the above methods should provide an adequate source of information from which to base the Business Continuity Plan. All relevant information should be stored for reference for at least one year or until the next BIA.

(v) Business Impact Analysis (BIA's) must be signed off by department or functional heads through a formal functional process stipulating that they understand, accept and verify BIA's are correct.

O. Recovery Procedures

(i) The business continuity plan should address staff requirements and relocation to the alternate site in the event of a major disruption. A detailed list of tasks for offsite recovery should be made available to all concerned staff

(ii) NCWSC business continuity management team should:
(a) Identify those business functions and operations to be recovered on a priority basis and establish recovery procedures
(b) Establish recovery procedures proportional to the risk they pose to the financial system.
(c) There are measures for the quality of planning, competency of staff and effectiveness of the business continuity plan.
(d) There is organizational awareness of emergency procedures and team members and staffs are familiar with their roles, accountability, responsibilities and authority in response to an incident.
(e) All technological, logistical and administration aspects of the business continuity plan have been tested.
(f) The recovery of infrastructure including command centers and off site work area is assured.
(g) The availability and relocation of staff is assessed
(h) An inventory of assets needed for offsite recovery should be generated
(i) The alternate site should be sufficiently equipped with the necessary equipment, data and to maintain critical operations and services for a sufficient time period

(iii) Methods and Techniques
Management should develop a test plan for each BCP testing method used. NCWSC should employ various methods of exercising including but not limited to the following
(a) Technical tests
(b) Desktop /Orientation/walkthroughs
(c) Live runs
(d) Simulations
(e) Integrated tests for departments that are dependent on each other and also stress testing of recovery facilities

(iv) Communication
NCWSC should include in its business continuity plans procedures for communicating within the Company and with relevant external parties in the event of major disruptions. The Company shall ensure that the response to a disruption is communicated internally and externally to applicable parties. External communication to the media must only be through the external communications teams and approved by senior management or the Company

(v) The communication procedures should:

(a) Ensure that there is a clear plan identifying staff, for communicating internally (within the organization) and externally (to the public) stakeholders

(b) Establish communication protocols clearly outlining the chain of command from the Company, membership and stakeholders

(c) Develop a directory for all recovery team members including the crisis management and emergency management teams, local emergency response organizations and critical service providers.

(d) Ensure that the directory/contact lists are made available to all team members

(e) Address obstacles that may arise due to failure in primary communications systems (electricity, mobile phone network, road network). Ensure that the institution has set up alternative modes of communication

(f) Ensure that copies of business continuity plans are disseminated to the relevant personnel

ANNEX II: ACKNOWLEDGEMENT OF ICT SECURITY POLICY

I have read and understood the Company's ICT security policy. I will adhere to the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

ACCEPTANCE

Name: _____ Man Number: _____

Signature: _____

Date: _____