THE NELSON MANDELA

AFRICAN INSTITUTION OF SCIENCE AND TECHNOLOGY

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY AND OPERATIONAL PROCEDURES

March, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document presents the Information and Communication Technology (ICT) Policy and Operational Procedures of the Nelson Mandela African Institution of Technology (hereinafter referred to as “NM-AIST” or “the Institution”). The document stipulates policy statements and standard operational procedures on critical ICT areas, and the regulations to enable their implementation. In formulating this Policy, the institution has tapped into the experience of other comparable Institutions and made references to international best practices in ICT. The views from both the internal and external stakeholders have also been incorporated.

Being an institution on Science, Engineering, Technology and Innovation, and one of it’s kind in the region, there are vast opportunities to develop exquisite ICT infrastructure for applications and systems that are necessary for accomplishing world-class learning and research environments, and seamless communications. Recognizing the opportunities and the potentials that come along with observing best practices when using ICT, the objective of this policy is to ensure that all ICT resources of the Institution are procured, efficiently and effectively operated, used and disposed (when necessary) in a manner that does not compromise security, integrity, confidentiality and continual availability of services. Security, integrity, confidentiality and ever-ready services will guarantee positive impact of ICT on the institution’s corporate vision and mission. By understanding that it is very essential to build on achievements which have already been made, special emphasis is put on areas where achievements have been less and on strengthening the identified weakness areas.

In order to promote greater uptake of ICT within the institution, and simplify readability of this document, the policy is organized in three distinct and critical areas of ICT: **Network and Infrastructure**; **Systems and Applications**; **Software and Data and Extending Services to External Clients**. For each area, we present the policy issue, objectives, statement, and the standard operating procedures. We also present how this policy can be implemented in Chapter 6 and the detailed guidelines and regulations in Chapter 7.

This policy will provide a comprehensive framework for the effective deployment and use of ICT in driving the core businesses of the institution.

ACRONYMS AND ABBREVIATIONS

Word	Meaning
IT	Information Technology
ISP	Internet Services Provider
ICT	Information and Communication Technology
OEM	Original Equipment Manufacturer
PC	Personal Computer
PMU	Procurement Management Unit
PPA	Public Procurement Act
CA	The Cybercrimes Act
AIA	Access to Information Act
ETA	Electronic Transactions Act
PPR	Public Procurement Regulation
NM-AIST	Nelson Mandela African Institution of Science and Technology
UPS	Uninterruptible Power Supply
VPN	Visual Private Network
HDD	Hard disk
COBIT	Common Objectives for Information and related Technology
ITIL	Information Technology Infrastructure Library
ISO	International Standards Organization
LAN	Local Area Network
NIC	Network and Infrastructure Committee
SAC	Systems and Application Committee
SDC	Software and Data Committee

INTERPRETATIONS OF TERMS

Word / Phrase	Meaning
Access Controls	Means of establishing and enforcing rights and privileges of users.
Access Rights	Authorized entry into a computer system to read, write, modify, delete or retrieve information contained therein.
Act	The law under which the Nelson Mandela African Institution of Science and Technology (NM-AIST) was established.
Application Software	Computer software designed to perform a defined business function.
Audit Trail	A trailing mechanism on what was done, when, by whom and what was affected.
Authentication	Mechanism of verifying the identity of user.
Authorization	Enabling specification and the subsequent management of allowed actions for a given system. ICT relies on identification and authentication and enables access control.
Availability	The assurance that information / data are available on a timely basis wherever / whenever ICT is needed to meet Institutional requirements or to avoid substantial losses.
Compliance	To act according to certain accepted standards or rules.
Computer Network	A collection of computers and devices interconnected in order to enable resource sharing.
Confidentiality	The protection of information from unauthorized disclosure.
Data Backup	A process whereby data or programs in a computer are copied to storage media for possible future restoration.
Data Recovery	A process of loading copied data or programs back into the computer from the storage media.
Data	Basic facts and figures that can be processed to useful information.
Database Administration	The role generally associated with the management and control of a Database.
Database	A collection of data that is organized so that ICTs contents can easily be accessed managed and updated to serve multiple uses.
Department	Means a unit as described in NM-AIST's Organizational structure.
Email System	All means of sending, receiving and storing electronic mails (e-mails).
Employee	A person employed by the Institution on permanent or contractual terms.
Encryption	Conversion of messages (data / voice / video) into a form that cannot be understood by unauthorized readers.
End user	All Users of ICT Systems including Systems developers and Administrators.

Word / Phrase	Meaning
Executive Management	It is a body that involves the Vice Chancellor, Deputy Vice Chancellor-Academic Research & Innovation and Deputy Vice Chancellor- Planning, Finance and Administration.
Guidelines	Acceptable approach in implementing a policy or procedure.
Head	An officer in-charge of a Department.
ICT Equipment	Tangible computer assets, such as computer hardware, network or communication devices including laptops, personal computers, servers, printers and scanners, firewalls, digital cameras, modems, and UPS.
ICT Resources	ICT Equipment together with operating procedures manuals, user guides and computer output.
Identification	The process of distinguishing one user, process or resource from another.
Information& Communications Technology (ICT)	A generic term used to express the convergence of Information and Communication Technology, broadcasting and communications.
Information Security	Means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
Information System	The term that encompasses all components required for the processing of information e.g. Applications, Databases, Operating Systems and Network Components.
Information	Processed data that provide useful meaning to the Institution.
Institution	Nelson Mandela African Institution of Science and Technology (NM-AIST) established under the Universities Act, No 7 of 2005 as one in a network of African Institutes of Science and Technology (AIST) in Sub-Saharan Africa (SSA).
Integrity	The protection of information / data from unauthorized, unanticipated or unintentional modification or deletion, or to be able to identify such action when ICT cannot be prevented.
Intel Processors	A brand of computer processors from Intel Company.
Internet	A publicly accessible 'network of networks' connecting users and Institutions worldwide.
Intranet	A private version of Internet, normally involving one organization with the main purposes of enabling information sharing.
Malicious codes	A new breed of Internet threats that cannot be efficiently controlled by conventional antivirus software alone.
Management	The Institution’s Management Team consisting of Deans of Schools and Heads of Departments.
Mass Storage Device	Device that can store large amounts of information.
Mass-mail	E-mail sent to more than one recipient at a time.
Network Administration	The role generally associated with the management and control of computer networks.

Word / Phrase	Meaning
Network equipment	Any devices that facilitate or enhance data communication and includes routers, switches, hubs, firewalls, switches and cables.
Policy	Governance instrument and approved by the Council on strategy and direction that identifies and defines specific areas of concern and states the organization's position.
Premises	Institution's buildings with ICTs outbuildings, land and property registered in the name of, or leased by the Institution.
Procedure	Detailed steps to be followed to accomplish a particular task or to achieve specific results.
Rack	Standard device for holding ICT equipment in a stack.
Regulations	A rule or directive made and maintained by an authority.
Server	A powerful computer used for centralized data storage and processing of data.
Software Development tools	Software and tools used in system development.
Software piracy	The utilization of software in violation of ICTs licensing agreement.
Software utilities	These are small computer programs that provide an addition to the capabilities provided by the operating system.
Software	Computer programs including operating systems, applications, utilities and accompanying documentation.
Staff Regulations	The Institution Staff Regulations.
Standards	Specified uniform use of tools, techniques and methods to implement a policy or procedure.
System Administration	The role associated with the management and control of operating system and ICTs associated hardware.
System Integrity & Recoverability	These are means that ensure that processing of information resources behave in an appropriate or predefined manner in accordance with business processes. It also means providing mechanisms to detect, prevent and correct the unauthorized modification, insertion, deletion or replay of information.
Systems	Computer Systems.
Third Party	An individual or legal entity explicitly authorized by the Institution, including consultants, contractors, vendors, agents, and personnel affiliated to them.
Users	Include Institution's employees, students, temporary workers, external contractors, consultants, external auditors or any other parties which entered into an agreement to provide a service to the Institution and obtain access to Institution's information systems and use Institution's systems.
Vice Chancellor	The Chief Executive Officer of the NM-AIST responsible for overall management of the operations of the institution.

Word / Phrase	Meaning
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user, and often causes damages to systems or data.
Webmaster	Person responsible for updating, designing, developing, marketing and maintaining website.

CHAPTER 1

INTRODUCTION

1.1 Background

The Nelson Mandela African Institution of Science and Technology (NM-AIST) was stablished in 2009 under the Tanzania's University Act, 2005. It is part of the network of Pan-African Institutions of Science and Technology located across the continent. The institution is aiming to contribute substantially to the training of a critical mass of world-class scientists, engineers and technologists for Africa's economic and technological transformation. It is being developed into a research intensive institution for graduate and post-doc studies and research in Science, Engineering, Technology and Innovation (SETI). The institution has been setup to build capacity to achieve among other things; generation and transformation of knowledge into tangible products and industrial and business solutions, and promotion of the application of technology to generate wealth. Furthermore, NM-AIST seeks to establish a world-class environment for research and technology development and to build capacity to generate and apply knowledge for sustainable development; and to produce the required value-added human capital for development.

To achieve its vision and mission, NM-AIST is looking into extensively utilizing Information and Communication Technology (ICT) to support its business processes including teaching and learning, and research and innovation. Therefore, it is critical that NM-AIST devise a policy which guides how ICT is used and is in line with other governmental initiatives including the National ICT Policy developed in 2003. At a global level, institutions have adopted COBIT, ITIL and ISO for the facilitation of alignment of all ICT developments, management and operations with their corporate strategies, putting in place best practices, processes, policies, programmes (strategic road maps) and appropriate structures and organization which empower the leadership and ensure that all key decisions related to ICT are made with the appropriate information and at the right level and time. It is within the same context that NM-AIST has formulated this ICT Policy to cover key aspects of information and related technologies.

Within its few years of existence NM-AIST has put in place a number of information systems to support delivery of its services and products. The level of investment and ICT dependency that the Institution has on achieving its goal and objective has grown significantly. However, the biggest challenge is to ensure that the institution's businesses and ICT are moving in the same direction. The need for proper ICT governance is thus of paramount importance and for which this Policy to address. The policy has been formulated with the various national Acts in mind. It complies with and falls within the framework of the rights and access to information, the AIA 2015. It recognizes incidences which constitute crimes as stipulated in the CA 2015 and the ETA 2015.

1.2 NM-AIST Vision

To become a world class institution of higher learning dedicated to pursuit and promotion of excellence in science and engineering and their application for economic growth and sustainable development in Africa.

1.3 NM-AIST Mission

To deliver and promote high quality and internationally competitive teaching and learning, research and innovation, and public service in science, engineering and technology leverage on entrepreneurship for enhanced value addition to people and natural resources, with a view to stimulating, catalysing and promoting economic growth and sustainable development in Tanzania and Sub-Saharan Africa.

1.4 Objectives of NM-AIST

1.4.1 General Objectives

The general objects of the Institution are the advancement of knowledge and creativity; the diffusion and extension of the science and technology; the provision of higher education, research and innovation that incorporates outreach and public service; and, so far as is consistent with those objects, the nurturing of the intellectual, aesthetic, social and moral growth of the students at the University.

1.4.2 Specific Objectives

To advance learning and knowledge aiming at producing high quality scientists and engineers through teaching and learning, research and innovation, extension and public service in science, engineering and technology, business studies and humanities, and their applications for sustainable socio-economic development in Tanzania and Sub-Saharan Africa.

1.5 Organization Structure and Services Managed at NM-AIST

The ICT Resources Centre (ICT-RC) has the following organization structure as shown in Figure 1. The NM-AIST community has access to limited ICT services that are administered by the ICT-RC. The services include electronic mailing using a third party mailing exchange, Internet, name resolution services using a third party Domain Name Server (DNS), Information Systems, lecture and meeting rooms presentation support, the institution website, library systems, WIFI hotspots and landline phones. A SWOT analysis was conducted on the current situation and below were the findings.

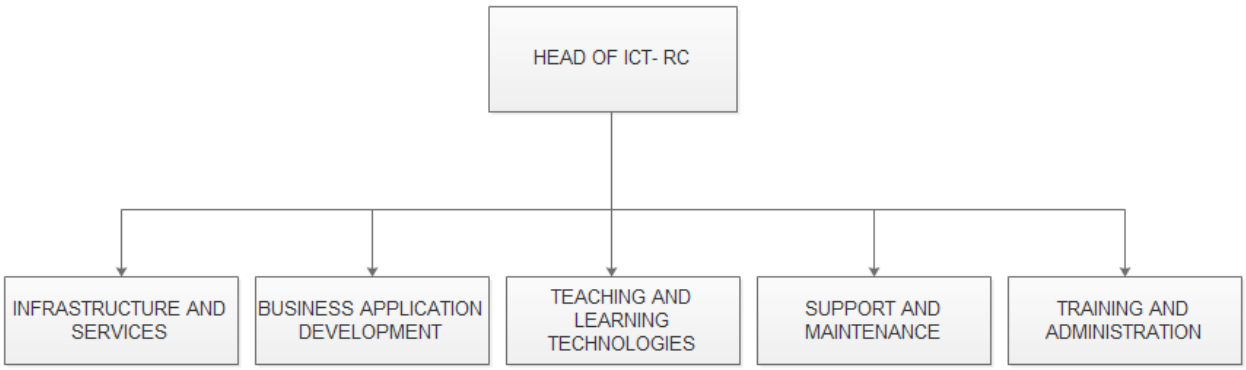


Figure 1: Organization Structure of ICT-RC

1.5.1 Strengths

1. The presence of large proportion of average to advanced ICT users.
2. The presence of the School of Computational and Communication Sciences and Engineering (CoCSE).
3. Special status of the Institution.
4. People working in close proximity.

1.5.2 Challenges and weaknesses

1. Lack of internet back-up.
2. Lack of service level agreement for maintenance and repair of ICT facilities.
3. Lack of offsite back-up system.

1.5.3 Opportunities

1. Advances in technology e.g. cluster computing, cloud computing.
2. Systems could be integrated for better performance and control.
3. Availability of the state-of-the-art solutions.
4. Access to the best IT management practices.

1.6 The need for ICT Policy

As a public institution, NM-AIST is required by law to have policies including one on ICT. This is because, ICT policy in particular, is key for the protection and guidance of the institution and its members by providing them with rules and guidelines for acceptable use of ICT resources and facilities. Apart from this law-bound need for ICT policy, it is very much in the institution's own interest to have one for many other reasons including:

- Manifestation of the impacts of ICT requiring guided use of the resources.
- Convergence and changing roles of ICT.
- Reducing the risk posed onto the assets of the institution as their management complexity increases.

1.7 Goal of the ICT Policy

The goal of this policy is to enable the NM-AIST to earn credibility from the ICT world by having quality and effective ICT practices as the foundation of success, in terms of achieving its corporate vision and mission.

1.8 ICT Policy Objectives

The general objective of the ICT Policy is to safeguard the integration of ICT which aim at enhancing access to computing and storage resources, and communication, with the view of achieving the corporate vision and mission of the institution.
To realize the general objective, the following specific objectives have been formulated:

1. To ensure that all ICT resources of the Institution are efficiently and effectively operated, used and disposed (when necessary) in a manner that does not compromise security, integrity, confidentiality and continual availability of services.
2. To strategically align ICT with the business and collaborative solutions.
3. To enhance value delivery, concentrating on optimizing cost-effectiveness and providing the value of ICT.
4. To ensure best risk management practice by safeguarding the ICT assets during disaster, smooth disaster recovery, and continuity of operations.
5. To effectively manage ICT resources and optimized acquisition and application of knowledge.

1.9 Scope of the Policy

The policy is developed to cover all business functions of the Institution. The policy aligns ICT strategy with the institution's Corporate Strategy. The policy will centrally focus on the four domains under the international ICT governance framework (COBIT) namely: planning and organization of ICT; acquisition and implementation of ICT assets; delivery and support of ICT services; and monitoring and evaluation of ICT performance.

1.10 Policy Issues and Statements

This policy is presented in three ICT areas (network and infrastructure; applications, systems and services; and software and data) which have been organized in a horizontal fashion in relation to the ICT governance framework. That is, each specific area constitute part of planning and organization of ICT; acquisition and implementation of ICT assets; delivery and support of ICT services; and monitoring and evaluation of ICT performance.

For each of the three areas, policy issue, policy objectives, policy statements and operational procedures are organized into a Chapter. These form chapters two, three and four. In Chapter Five, the document outlines a framework on which the above policy shall be implemented. Chapter Six presents general guidelines and regulations.

CHAPTER TWO

NETWORK AND INFRASTRUCTURE

2.1 Policy Issue

Network and infrastructure refer to the physical network and all facilities which offer connectivity, computational, communication and storage services. Network and infrastructure constitute networking resources (LAN Installation, switches, routers, access points, etc.), computing and communication resources (servers, telephones, projectors etc.), facilities (laboratories, conference rooms, etc.) and other resources (UPSs, card readers etc.) which are usually used by all sorts of users including academic staff, administrative staff, students, research fellows and guests. Apparently, the resources, users and users' ICT knowledge are very diverse. Without proper use, coordination, clearly mandated personnel for administering and performance monitoring the network and infrastructure, and well defined procedures, it is impossible to secure and sustain them, and ensure that their impact is felt.

2.2 Policy Objective

To ensure that the network and infrastructure of NM-AIST support the teaching and learning, and research and innovation related activities of the institution in a manner that does not compromise availability of services, security, integrity, and confidentiality.

2.3 Policy Statements

The Nelson Mandela African Institution of Science and Technology shall:

1. Mandate the DVC-ARI to oversee all network expansions, improvements, and operations, and the disposal of equipment when necessary.
2. Empower the ICT Resource Center to manage the NM-AIST network and infrastructure.
3. Strive to enhance network capacity and speed.
4. Establish a committee to assist the DVC-ARI in overseeing planning, development, operations and monitoring and evaluations ICT activities.
5. Develop sets of procedures and guidelines for secure and effective use, maintenance and disposal of parts of the network and infrastructure.
6. Strive to advance the knowledge and skills of the users.
7. Remain the owner of the network and infrastructure and retain the right to restrict or remove user's access right in case of misuse.
8. Ensure that the network and infrastructure is administered in ways that do not violate the national legislation including the Public Procurement Act 2011, the Cybercrimes Act 2015, Access to Information Act 2015 and Electronic Transaction Act 2015.

2.4 Operational Procedures

The Nelson Mandela African Institution of Science and Technology will:
:

1. Develop clear guidelines for operating and using the network and infrastructure in ways that do not compromise availability of services, security, integrity, and confidentiality. The guidelines should include how to handle private computational devices, procurement issues, disposal of parts of the network and infrastructure of NM-AIST.
2. Establish and empower the committee, which will primarily be composed of NM-AIST members with expertise in the field, and, additionally representatives from other units and/or departments.
3. Regularly educate all members of the institution about the guidelines.
4. Ensure that all members of the institution adhere to the guidelines.
5. Encourage all members to utilize the network and infrastructure to improve their work performances.
6. Develop strategies on how the institution should embark on enhancing capacity in order to increase the impact of ICT towards the institution's strategic goals and objectives.

CHAPTER THREE

SYSTEMS AND APPLICATIONS

3.1 Policy Issue

At NM-AIST, there are many systems and applications which offer various services which are aimed at enabling the institution's businesses. These include internet and intranet, electronic mailing system, Web services, academic systems (examination, repositories, anti-plagiarism, library, e-learning etc.), laboratory systems and management systems (accounts, payroll, human resource, asset management, etc.). For the institution to realize its vision and mission, it is critical that the systems and applications support the businesses seemingly, securely and with high availability and observed service level agreement. This requires dedicated organs which will embark on securely operating the systems and applications while observing service level agreements, strategic planning and organization of the systems, acquisition and implementation of new systems, and that applications support their operations and monitoring and evaluation. Therefore, a proper organ is necessary for the undertaking of duties pertaining to the businesses of NM-AIST.

3.2 Policy Objective

To ensure that the systems and applications which run in the institution's network and infrastructure are:

1. Implemented, operated, used and disposed (when necessary) in a manner that does not compromise security, integrity, confidentiality and continual availability of services.
2. Offering desired services at an international standard level, in terms of observing service level agreement, risk management, business continuity and change management.
3. Well managed and their operations smoothly continued during an emergency
4. Operated at a minimum risk, including licensing issues.

3.3 Policy Statements

The Nelson Mandela African Institution of Science and Technology shall:

1. Mandate the DVC-ARI to oversee while head of ICT-RC coordinates all deployments and operations of systems and applications that run in the NM-AIST network.
2. Empower the ICT Resource Center to administer the systems and applications that run in the NM-AIST network and infrastructure.
3. Establish a committee to assist the DVC-ARI in overseeing planning for expansions, and monitoring and evaluations activities.
4. The services offered by the systems and their applications shall undergo constant improvement to keep abreast with technological advances.

5. Develop sets of procedures and guidelines for secure and effective use, maintenance and decommissioning of systems and applications.
6. Strive to advance the knowledge and skill of systems and application users.
7. Embark on constant improvement of the services offered by the systems and applications.
8. Remain the owner of all systems and applications and retain the right to restrict or remove user's access right following a misuse.
9. Ensure that the Systems and Applications are administered in ways that do not violate the national Acts including the Public Procurement Act 2011, the Cybercrimes Act 2015, Access to Information Act 2015 and Electronic Transaction Act 2015.

3.4 Operational Procedures

The Nelson Mandela African Institution of Science and Technology will:

1. Develop clear guidelines for administering, running and using each system and/or application in ways that do not compromise availability of services, security, integrity, and confidentiality. The guideline should include procurement issues and software downloading. The key systems/applications include the electronic mailing systems, the Website, the intranet and internet, the examination system, laboratory systems, the library systems, the management systems (Accounts, HR, and procurement).
2. Develop guidelines on how to manage systems and applications that the individuals install and use.
3. Establish and empower the committee, which will primarily is composed of NM-AIST members with expertise in the field, and, additionally, representative from other units and/or departments.
4. Regularly educate all members of the institution about the guidelines.
5. Ensure that all members of the institution adhere to the guidelines.
6. Encourage all members to utilize the systems and applications to improve their work performances.
7. Develop strategies on how the institution should embark on enhancing capacity in order to increase the impact of ICT towards the institution's strategic goals and objectives. This includes maintaining a two-year running budget.

CHAPTER FOUR

SOFTWARE AND DATA

4.1 Policy Issue

Being an academic institution, NM-AIST community

1. Generates a lot of data, some of which are sensitive and confidential. This includes programs/software, research data, published materials, administrative data and e-materials.
2. Acquires a lot of software packages.

As the world now understands that data is the new gold in this century, NM-AIST must therefore ensure that there are policies and well defined guidelines on how to acquire, secure, and provide access to such data.

4.2 Policy Objective

To ensure that the programs/software and data which are stored in the institution's infrastructure do not pose any threat, have been lawful acquired, are secured, and there are proper guidelines to manage them in a way that contributes to the realization of the institution's strategic goals.

4.3 Policy Statements

The Nelson Mandela African Institution of Science and Technology shall:

1. Mandate the DVC-ARI to oversee while head of ICT-RC coordinates all acquisition and creation, storage and administration pertaining to software and data within the institution's infrastructure.
2. Establish a committee to assist the DVC-ARI in overseeing monitoring and planning for acquisitions, creation, storage and administration of software and data within the institution's infrastructure.
3. Ensure that use of, disposal of, and access to software and data within the institution's infrastructure shall be guided by sets of procedures and guidelines for security and effectiveness.
4. Provide a data storage space to each researcher within the institution's network and infrastructure.
5. There shall be an information officer as obliged by the National Access to Information Act 2015.
6. The network and infrastructure shall e managed in ways that do not violate the national laws as stipulated in the various Acts including the Public Procurement Act 2011, the Cybercrimes Act 2015, Access to Information Act 2015 and Electronic Transaction Act 2015.

4.4 Operational Procedures

The Nelson Mandela African Institution of Science and Technology will:

1. Develop clear guidelines for acquiring, storing, and managing (including access) software and data in ways that do not compromise availability of services, security, integrity, and confidentiality. The guidelines should include how to request for information from the information officer and how the information officer should handle such requests.
2. Request for information from people in and outside the institution shall be submitted to the designated information officer who will process the requests as per guidelines
3. Establish and empower the committee, which will primarily is composed of NM-AIST members with expertise in the field, and, additionally, representative from other units and/or departments.
4. Regularly educate all members of the institution about the guidelines.
5. Ensure that all members of the institution adhere to the guidelines.
6. Allocate departmental public storage spaces and private storage spaces.
7. Develop strategies on how the institution should embark on improving awareness on issues related to ethics and copy right.

CHAPTER FIVE

EXTENDING SERVICES TO EXTERNAL CLIENTS

5.1 Policy Issue

Being an academic institution, NM-AIST community

1. Develop a lot of data, software and systems of which other organization or institution can purchase or request to use.
2. Acquires a lot of ICT hardware such as ICT Testing Labs, Powerful server machines and High Performance Computing.

As the ICT issues changes drastically in this century, NM-AIST must therefore ensure that there are policies and well defined guidelines on how to acquire, secure, and provide an excellent service to the clients, contribute to national development and make the most efficient and effective use of resources.

5.2 Policy Objective

To ensure that the ICT services offered by the institution to external clients do not pose any threat, have been lawful acquired, are secured, and there are proper guidelines to manage them in a way that contributes to the realization of the institution's strategic goals.

5.3 Policy Statements

The Nelson Mandela African Institution of Science and Technology shall:

1. Mandate the DVC-ARI to oversee while head of ICT-RC coordinates all acquisition and creation, storage and administration pertaining to software, systems and data within the institution's infrastructure.
2. Establish a committee to assist the DVC-ARI in overseeing monitoring and planning for acquisitions, creation, storage and administration of software systems and data within the institution's infrastructure.
3. Ensure that use of, disposal of, and access to software, systems and data within the institution's infrastructure shall be guided by sets of procedures and guidelines for security and effectiveness.
4. Provide a backup storage space to software, systems and data within the institution's infrastructure.
5. The ICT services offered by the institution shall not violate the national laws as stipulated in the various Acts including the Public Procurement Act 2011, the Cybercrimes Act 2015, Access to Information Act 2015 and Electronic Transaction Act 2015.

5.4 Operational Procedures

The Nelson Mandela African Institution of Science and Technology shall:

1. A description of the ICT services and how thy will be delivered.
2. The monthly fees and deliverables attached to the fees if applicable.
3. The cost structure and payment schedule.
4. The period of contract, renewal and termination clauses.
5. Availability, reliability and capacity of person/s responsible fro delivering the service.
6. Confidentiality and non-disclosure.
7. In the case of software development:
    - Who owns the program as well as the ideas and processes that makes it a valuable piece of software within the environment.
    - Who is responsible for testing and ensuring that users are completely satisfied, as well as who is responsible for ensuring that users are able to use the software successfully.
    - Who is responsible for and how the software will be maintained in the future.
8. The responsibilities of both parties for ICT disaster recovery.
9. Describe serving reporting procedure and specification involvement of client's audit team.

CHAPTER SIX

POLICY IMPLEMENTATION

6.1 Introduction

Because of the multifaceted nature of the ICT issues and the factors that impact on them, the implementation of this policy, and the consequent achievement of its goals and objectives will be the responsibility of the entire institution at all levels and in all sectors. Active participation of all members of the institution, ICT-RC staff, and the head of ICT-RC, Deans of Schools, DVCs, VC, the Senate, and the Council is therefore very crucial.

This chapter outlines the policy implementation strategy and the roles and responsibilities which each of the above players shall play for the successful implementation of the policy. The strategy aims at enabling efficient implementation of the policy in ways that will help the institution realize the full benefits of the ICT.

6.2 Strategy

6.2.1 Strategic principles

- Institution-wise collective effort to implement the policy.
- Strong ICT leadership and a performance watchdog mechanism.
- Constant improvement of key areas.
- Strategic plans for ensuring continuity of the Institutions' businesses and activities.

6.2.2 Strategic areas of implementation

- Enhancing ICT management capacity.
- Enhancing infrastructure.
- Installation and expansion of the state-of-the-art network.
- Deployment of world class systems and applications.
- Fostering close collaboration between ICT-RC, the ICT Committee, and the School of CoCSE.
- Well-structured budgeting system.

6.3 The ICT-RC

ICT-RC is a unit within the institution that is responsible for the daily management and operations of the ICT resources. This unit directly reports to the VC.

6.3.1 Terms of reference

- Administer NM-AIST's network, and the systems and application that run in it.
- Give support to users of the ICT infrastructure and systems.

- Review all ICT services and applications including Institution's website and infrastructure, with the view to advise the Institution on required improvements; and ensure that the risks associated with ICT are managed appropriately.
- Follow all stipulated guidelines in managing the NM-AIST's network.
- Implement all measures stipulated in the guidelines in relation to service availability, security, integrity, and confidentiality.
- To give feedback on status and performance of the respective ICT resources

6.4 The Information Officer

The information officer is an officer to whom all application for information, which is under the custody of the institution, should be submitted. This officer will be appointed by the VC on two years tenure.

6.4.1 Terms of reference

- To process all request for information from inside and outside the institution.
- To regularly publish the details of the information that is under the custody of the institution for the purpose of creating awareness.

6.5 ICT-RC Board

The VC shall appoint ICT-RC Board whose composition shall be approved by the Council. The ICT-RC Board will serve to monitor the deployment, use, maintenance and performance of all ICT resources in adherence to the ICT policy and the institution's strategic goals and objectives. The board should be composed of the following

- The chairman, to be appointed by the VC.
- The information officer.
- One co-opted member, to be appointed by the committee chair.
- The head of ICT-RC.
- One representative from Schools/departments (one of them will be the secretary of the committee).
- Two ICT experts from outside the institution.

6.5.1 Terms of references

- To develop sets of guidelines and procedures as required by the ICT policy.
- To develop and review ICT strategies/plans that ensures cost effective operations of ICT. This includes working with IRC to establish a two-year running budget.
- To review current and future technologies in order to identify opportunities to increase the efficiencies of ICT resources.
- To monitor and evaluate ICT projects, including conducting network and systems audits.

- To ensure that ICT resources are efficiently used for academic, research and other purposes.
- To follow-up on recommendations of the ICT-RC board, and new ICT projects.
- Give advice on the best strategies for ensuring cost effective operations.
- To establish relevant service level agreements.
- Coordinate the establishment and continued review of NM AIST-Arusha's ICT Policy and Strategy;
- Ensure that the ICT strategy is aligned with NM AIST's Business Corporate Plans;
- Advise the Council in making considered decisions about the focus of ICT resources;
- To monitor and evaluate the quality of the ICT services as per service level agreement.
- To ensure that ICT strategies are aligned with wider government directions and policies.
- To provide advice and recommendations to the VC on critical ICT issues.
- To maintain and review a living NM-AIST ICT policy.

6.5.2 Roles and Responsibilities of Members

1. **Chairperson**
   - Overseeing the overall functioning of the committee.

2. **Head of ICT- RC**
   - Provide regular audit reports on network, systems, applications and software.
   - Represent IRC to the committee.
   - Respond to inquiries from the committee.
   - Plan and develop ICT security strategies;
   - Monitor adherence to the ICT Policy and the presence of potential threats and risks by conducting periodic ICT security reviews;
   - Keep abreast of ICT Security developments in respect of the ICT industry in general, and the Institution's systems in particular;
   - Initiate and recommend proposals to change, modify or improve the Policy; and
   - Recommend Procedures, Standards and Rules for effective implementation of the Policy.

3. **The Two ICT experts from outside**
   - To offer technical advice to the ICT Committee.

4. **School and Departmental representatives**
    - To represent the Schools and/or departments.
    - To bring feedback from the users.

CHAPTER SEVEN

GUIDELINES AND REGULATIONS

7.1 Network and Infrastructure

Category	Guidelines and procedures
General	(1) Unless otherwise specified, users must apply to use any part of the network or infrastructure by filling the form ICT1.1 (for personal use) or ICT1.2 (for group use). (2) Users are obliged to report any incident (e.g. malfunctioning) that is associated with any part of the network or infrastructure by either filling in the form ICT1.3 or reporting to the ICT-RC or any of the ICT-RC staff. (3) Server(s) and other sensitive heavy duty computing devices shall be kept in a secure, air conditioned rooms. (4) All entries to the Server room must be recorded and security camera must be installed to monitor all accesses. (5) Any unit/department of the institution operating a part of the institutions' network and infrastructure, should communicate their operational guidelines to the ICT-RC. (6) Users shall not allow non-NM-AIST members to use ICT resources assigned to them without prior authorization from the ICT-RC. (7) All equipment must be switched off properly before users leave their offices or when they are not in use unless otherwise demanded by their duties. (8) Power protection on equipment must not be by-passed without proper authorization by Head of ICT-RC. (9) All members of the NM-AIST community shall have access to a monthly schedule of all the facilities. (10) The NM-AIST community must be informed by either email or a poster when a facility is in use. (11) All found-lost items should be reported to the ICT-RC and the ICT-RC should clearly specify procedures of handling the items. (12) There shall be regular network audits. Every time an audit is conducted, a report must be submitted to Senate through the ICT-RC Board.
Security	(1) ICT-RC must conduct physical inspections of the network and infrastructure quarterly, and submit reports to the VC. (2) Users of electronic devices that are connected to the institution's network or infrastructure must ensure that their

Category	Guidelines and procedures
	systems (i.e. operating system and other security applications) are updated regularly. (3) For any part of the network and infrastructure which requires authentication, passwords/pass phrase must be of a minimum length of six characters, and must contain a combination of numerals, letters and special characters. Those passwords should never be communicated by emails.
Access to resources	(1) Request to use any computing resource should be acted upon promptly. (2) Users should be provided with resources which meet their demands as necessitated by their duties.
Private devices	(1) Unless otherwise specified, permission to connect to the Institution's network and infrastructure must be sought from ICT-RC. (2) Users who connect their private devices to the institution's network and infrastructure should act responsibly by, for instance, ensure that their systems are updated and do not interfere with any other functioning of the network and infrastructure.
Procurement	The ICT-RC should assist the institution's PMU to establish the actual desired functionalities and devices, and identify the right supplier for the same.
E-waste	Prior to the disposal of any part of the network or infrastructure, permission must be sought from the ICT-RC Board and the ICT-RC should devise a disposal plan and conduct the disposal upon approval from the VC.
Capacity building	(1) The ICT-RC shall establish training needs of the users of the network and infrastructure. (2) The ICT-RC shall organize trainings and workshops to address the established needs.

7.2 Systems and Applications

Category	Guidelines and procedures
General	(1) Users have the right to install applications and systems, but only those which are approved by the ICT-RC Board. The ICT-RC shall therefore make the list of recommended applications available to all staff. (2) Users are obliged to report any incident (e.g. malfunctioning) related to the use of a system or application by sending an email to the Director of ICT-RC. (3) Authenticated users of systems should not share their authentication credentials with anyone. (4) Users shall not allow non-NM-AIST members to access the institution's systems and applications.

Category	Guidelines and procedures
	(5) Upon completing a task for which a systems or application was accessed, users are obliged to log-out completely. (6) There shall be regular systems and applications audits. Each time an audit is conducted, a report must be submitted to the ICT-RC Board.
Security	(1) Passwords/pass phrase must be of a minimum length of six characters. They must contain a combination of numerals, letters and special characters. (2) Users are not allowed to use same password for more than one (1) application or system. (3) Passwords should not be communicated through emails. (4) Applications and systems must be set to sign-out if idle for more than 15minutes. For systems which cannot do automatic sign-out, users are obliged t sign-out when leaving office.
Access to resources	(1) Request to use any computing resource should be acted upon promptly. (2) Users should be provided with resources which meet their demands as necessitated by their duties.
Electronic Mailing System	(1) Users are strictly prohibited from sending harassing, discriminatory and politically motivated messages. (2) Access to group mailing list should be restricted to only the concerned personnel. (3) No user should be given access to send emails to all users unless permitted by the ICT-RC. (4) After completion of student academic year, students shall be given a maximum of two months before closure of the student E-mail address.
Website	Anyone wanting to post information on the Website, must do so by filling in an application form (ICT2.1) or request permission from the Director of ICT-RC, detailing the information.
The internet	Any illegal downloads, by national and international laws are strictly prohibited.
Examination system	The academic office shall provide guidelines and procedure on how the examination systems are to be administered.
Laboratory systems	Each laboratory shall develop operational guidelines in collaboration with the ICT-RC and the relevant Laboratory Management Committee.
Library systems	In collaboration with the ICT-RC, the Library shall set guidelines and procedures on how to access library systems.

Category	Guidelines and procedures
Management systems	In collaboration with the ICT-RC, administrative units shall set guidelines and procedures on how to administer and use their respective systems.
Procurement	The ICT-RC shall assist the institution's PMU to establish the actual desired functionalities and devices, and identify the right supplier for the same.
E-waste	Prior to the disposal of any part of the network or infrastructure, permission must be sought from the ICT-RC Board, and the ICT-RC should devise a disposal plan and conduct the disposal upon approval from the VC.
Capacity building	(1) The ICT-RC shall establish training needs of the users of the network and infrastructure. (2) The ICT-RC shall organize trainings and workshops to fulfill the established needs.

7.3 Software and Data

Category	Guidelines and procedures
General	(1) The ICT-RC must avail spaces to all users for storage of software and data. (2) Users are strictly prohibited from misusing spaces which are allocated to them. (3) Users are prohibited from keeping illegally acquired software and data into the institution's infrastructure. (4) Systems and data backup must be performed daily, weekly and monthly in a manner that will ensure no loss in the event such backed-up data are required. (5) Backup storage of the same data must be done on two separate media and stored in physically separate locations to be specified by the Director of ICT-RC. (6) Users shall be assisted by the ICT Administrators to back up their individual information in their respective computers at least once every month. (7) The Head of ICT Resource Centre must ensure that all strategic information systems are stored in the Server and are backed up regularly. (8) NM-AIST Management must provide resources to allow for disaster recovery procedures. (9) Regular backup to all data stored within the fileserver of the institution's network should be made. Upon backup, a report must be submitted to the Director of ICT-RC by filling the form ICT1.6.

Category	Guidelines and procedures
Security	(1) Password used shall not be based on personal information such as year of birth, family name etc. (2) All user passwords must be changed at least once every six (6) months. (3) Any user who discover abnormalities, errors or loopholes in the system must report to the Head of ICT Resource Centre. (4) Users shall regularly update their antivirus and the ICT-RC shall ensure that computers are installed with up-to-date versions of antivirus. (5) Systems and data backup must be performed daily, weekly and monthly in a manner that will ensure no loss in the event such backed-up data are required. (6) Backup storage of the same data must be done on two separate media and stored in physically separated locations to be specified by the Head of ICT-RC. (7) Audit trail must be activated for all servers and must be checked on regular basis. (8) All Third Party Support shall sign confidentiality forms and supervised by ICT-RC.
Access to software and data	All request for information hosted within the institution's infrastructure should be made through the information office of ICT-RC
Software	The software stored in the infrastructure must be free of components which are harmful to the institution.
Research data	Research data should be kept in a well-organized manner which is also descriptive.
Published material	ICT-RC must conduct physical inspection of the network and infrastructure quarterly, and submit reports to the ICT-RC Board.
Administrative data	(1) No data shall be transferred, given or distributed to any institution or individual without authorization from the council. (2) Any division within the institution that creates any information or data shall be the owner of such information or data and shall be responsible for ICT's integrity and confidentiality.
Online and e-books	(1) All users must read or download book that the institution has access permission. (2) Author's guidelines and procedures should be followed if provided before downloading or using a book.
Ownership	(1) All Information and data processed, created, generated and stored in the Institution's computer facilities shall remain the property of the Institution.

Category	Guidelines and procedures
	(2) Any Division within the Institution that creates any information or data shall be the owner of such information or data and shall be responsible for ICTs integrity and confidentiality. (3) No information shall be transferred, given or distributed to any Institution or individual without authorization from the Senate. (4) All software developed by the Institution shall be the exclusive property of the Institution, and shall not be transferred, given or distributed to any Institution or individual without the written authorization of the VC of NM-AIST. (5) All software licensed to the Institution shall not be transferred, given or distributed to any Institution or individual.

CHAPTER EIGHT

APPENDICES

8.1 Declaration by Users

These declarations have been designed to certify that users acknowledge that they are aware of the Institution's Information and Communication Technology Policy and agree to abide by its terms.

(Declaration by NM-AIST Employee)

I, _____ (full name) acknowledge that the Institution's ICT Policy and Operational Procedures have been made available to me for adequate review and understanding. I certify that I have been given ample opportunity to read and understand it, and seek clarification about my responsibilities on it. I am, therefore, aware that I am accountable to all its provisions; and that I shall abide by them. I also understand that failure to abide by them; the Institution shall take against me appropriate disciplinary action or legal action, or both, as the case may be.

Signature: _____

Department/School:

_____

Job Title: _____

Date: _____/_____/_____

8.2 Declaration by Third Party

I, _____
of

_____
(name of your company and full address) do hereby acknowledge that the Institution has provided me with adequate time to review and understand its ICT Policy regulations. I am therefore aware of ICTs terms and requirements. I do hereby undertake, on behalf of my organization, regardless of my current employment status, to be responsible to, and abide by them. I also understand that any failure to abide by the Policy shall result in appropriate legal actions being taken against me or my Institution, or both, as the case may be.

Signature: _____

Job Title: _____

Date: _____/_____/_____

8.3 Website Disclaimer

The information contained on this website is provided in good faith, and every reasonable effort is made to ensure that it is accurate and up to date. Accordingly, this information is provided 'as is' without warranty of any kind. The Nelson Mandela African Institution of Science and Technology excludes all warranties, either express or implied (including but not limited to any implied warranties of merchantability, fitness for a particular purpose, satisfactory quality or freedom from hidden defects).

In no event shall the Nelson Mandela African Institution of Science and Technology be liable for any damage arising, directly or indirectly, from use of the information contained in this website including damages arising from inaccuracies, omission or errors.

Any person relying on any of the information contained in this website or making any use of information contained herein shall do so at his/her own risk. The Nelson Mandela African Institution of Science and Technology hereby disclaims any liability and shall not be held liable for any damages including, without limitation, direct, indirect or consequential damages including loss of revenue, loss of profit, loss of opportunity or other losses. The information contained in this website may be changed or updated at any time without notice.

In addition, links may be provided from this website to other websites which are not owned or controlled by the Nelson Mandela African Institution of Science and Technology. Please be aware that the Nelson Mandela African Institution of Science and Technology is not responsible for privacy practices of such other websites, and that when such links are selected, the user shall be leaving NM AIST website and be bound by privacy policy of those website.

8.4 E-mail Disclaimer

This e-mail message shall not be construed as legally binding on the Nelson Mandela African Institution of Science and Technology (NM AIST). As internet communications are not secure, NM AIST does not accept responsibility for the content of this message.

This message is intended only for the recipient(s) named above. Any unauthorized disclosure, use or dissemination, either in whole or in part, of this message is prohibited. If you have received this message in error, please inform the sender immediately by return e-mail and delete this message and any attachments thereto from your system.

8.5 Forms

8.5.1 Form ICT1.1: Access to Network and Infrastructure (Personal)

THE NELSON MANDELA

AFRICAN INSTITUTE OF SCIENCE AND TECHNOLOGY

(NM AIST)

ACCESS TO NETWORK AND INFRASTRUCTURE (PERSONAL)

REQUESTOR DETAILS

NAME: _____ E-MAIL: _____

EXTENSION: _____ DEPARTMENT NAME: _____

INCIDENT DETAILS

TYPE OF INCIDENT	TICK (where applicable)	SPECIFY THE REQUEST
Network		
Infrastructure		
Location of access		
Date of access		

ICT-RC OFFICER DETAILS (INCHARGE)

NAME _____ SIGNATURE _____

NETWORK AND INFRASTRUCTURE STATUS (EXPLANATION ON THE SOLUTION IF ANY)

8.5.2 Form ICT1.2: Access to Network and Infrastructure (Group)

THE NELSON MANDELA

AFRICAN INSTITUTE OF SCIENCE AND TECHNOLOGY

(NM AIST)

ACCESS TO NETWORK AND INFRASTRUCTURE (GROUP)

REQUESTOR DETAILS

NAME/ GROUP NAME _____ E-MAIL: _____

EXTENSION: _____ DEPARTMENT NAME: _____

INCIDENT DETAILS

TYPE OF INCIDENT	TICK (where applicable)	SPECIFY THE REQUEST
Network		
Infrastructure		
Location of access		
Date of access		

ICT-RC OFFICER DETAILS (INCHARGE)

NAME _____ SIGNATURE _____

NETWORK AND INFRASTRUCTURE STATUS (EXPLANATION ON THE SOLUTION IF ANY)

8.5.3 Form ICT1.3: Incident Reporting

THE NELSON MANDELA

AFRICAN INSTITUTE OF SCIENCE AND TECHNOLOGY

(NM AIST)

INCIDENT REPORTING FORM

REQUESTOR DETAILS

NAME: _____ E-MAIL: _____

EXTENSION: _____ DEPARTMENT NAME: _____

INCIDENT DETAILS

TYPE OF INCIDENT	TICK (where applicable)	REASON(S)
Networking and Infrastructure		
Application and Systems		
Software and Data		
Location of incident		
Date of incident occurrence		

ICT-RC OFFICER DETAILS (INCHARGE)

NAME _____ SIGNATURE _____

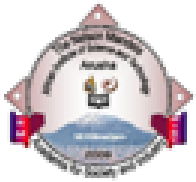
INCIDENT STATUS AND EXPLANATION ON THE SOLUTION USED

8.5.4 Form ICT1.4: Network Audit Report

THE NELSON MANDELA

AFRICAN INSTITUTE OF SCIENCE AND TECHNOLOGY

(NM AIST)



NETWORK AUDIT REPORT

NAME/ TITLE.....

NETWORK AUDIT PROCESS DETAILS

DATE OF NETWORK AUDIT / TIME OF NETWORK AUDIT

TYPE OF NETWORK AUDIT

NUMBER OF GENERATION

EXTENT OF NETWORK AUDIT (Files/ Directories)

DATA MEDIA ON WHICH OPERATIONAL NETWORK AUDIT DATA ARE STORED

NETWORK AUDIT HARDWARE AND SOFTWARE (include version number)

STORAGE LOCATION OF NETWORK AUDIT COPIES

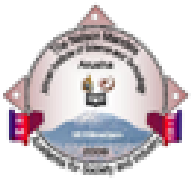
ICT-RC OFFICER'S SIGNATURE

8.5.5 Form ICT1.5: System Audit Report

THE NELSON MANDELA

AFRICAN INSTITUTE OF SCIENCE AND TECHNOLOGY

(NM AIST)



SYSTEM AUDIT REPORT

NAME/ TITLE.....

SYSTEM AUDIT PROCESS DETAILS

DATE OF SYSTEM AUDIT / TIME OF SYSTEM AUDIT

TYPE OF SYSTEM AUDIT

NUMBER OF GENERATION

EXTENT OF SYSTEM AUDIT (Files/ Directories)

DATA MEDIA ON WHICH OPERATIONAL SYSTEM AUDIT DATA ARE STORED

SYSTEM AUDIT HARDWARE AND SOFTWARE (include version number)

STORAGE LOCATION OF SYSTEM AUDIT COPIES

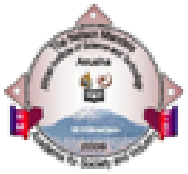
ICT-RC OFFICER'S SIGNATURE

8.5.6 Form ICT1.6: Data Backup Report

THE NELSON MANDELA

AFRICAN INSTITUTE OF SCIENCE AND TECHNOLOGY

(NM AIST)



DATA BACKUP REPORT

NAME/ TITLE.....

BACKUP PROCESS DETAILS

DATE OF DATA BACKUP/ TIME OF DATA BACKUP

TYPE OF DATA BACKUP

NUMBER OF GENERATION

EXTENT OF DATA BACKUP (Files/ Directories)

DATA MEDIA ON WHICH OPERATIONAL DATA ARE STORED

DATA BACKUP HARDWARE AND SOFTWARE (include version number)

STORAGE LOCATION OF BACKUP COPIES

ICT-RC OFFICER'S SIGNATURE
