INFORMATION AND COMMUNICATION TECHONOLOGY POLICIES

N.L.M.

NYANDENI LOCAL MUNICIPALITY

Type	Policy
Name	ICT policies • ICT risk management policy- review • ICT vendor and SLA management - new • Change control management- review • ICT security management- new • User account management- review • ICT asset management- new • Business and ICT continuity- new • Data backup and restore- new • ICT capacity planning and availability management • Incident and problem management- new
Classification	Internal Use Only
Owner	Senior Manager Corporate Service
Custodian	Senior Manager Corporate Service
Approved by	
Approval Date	
Effective Date	

Classification

This document has been issued strictly for internal purposes of Nyandeni Local Municipality

Copyright

TABLE OF CONTENTS

Definition of Terms

- **ISO/IEC 38500:** Internationally accepted as the standard for Corporate Governance of ICT; it provides governance principles and a model.
- **ISO 27002:2013** Information technology — Security techniques — Code of practice for information security controls.
- **Network:** is a platform that enable the sharing of files and information between multiple systems.
- **SLA:** Service Level Agreement.
- **Storage medium:** is a device for recording/storing information or data.
- **BIA:** Business Impact Assessment.
- **PC:** Personal computer
- **ICT:** Information and Communication Technology
- **User:** a person who uses a computer or any ICT equipment and systems
- **MCGICT:** Municipal Corporate Governance of Information and Communication Technology
- **COBIT:** Control objectives for Information and related technologies- An internationally accepted process framework for implementing Governance of ICT.
- **ITIL:** Information Technology Infrastructure Library - a set of detailed practices for ICT service management that focuses on aligning ICT services with the needs of business.
- The King IV report: The most commonly accepted corporate governance framework in South Africa.

1 INTRODUCTION

The advancement of Information and Communication Technology (ICT) has brought about rapid changes in the way businesses and operations are being conducted in the financial industry. ICT is a key enabler for business strategies including reaching out to and meeting external customer needs. As technology becomes increasingly important and integrated into business processes, the need for adequate and effective governance and management of both ICT resources and any constraints becomes imperative.

Both hardware and software assets and facilities have significant value and require the efficient and effective management and oversight to ensure that they are managed appropriately throughout their lifecycle.

2 OBJECTIVES

To implement best practices by using ICT policies and procedures in the computer and network environment. To enhance consistency and establishing clear criteria for computer and network hardware, software, ICT security, and vendors.

3 SCOPE

This policy applies to all Nyandeni Municipality employees and councillors. It is the responsibility of all operating departments to ensure that these policies are clearly communicated, understood and followed. These policies cover the usage of all of the municipality's ICT resources, including, but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, workstations, wireless computing devices, telecomm equipment, networks, databases, printers, Servers and shared computers, and all networks and hardware to which this equipment is connected.
- All electronic communications equipment, including telephones, 3G cards, e-mail, fax machines, wired or wireless communications devices and services, Internet and intranet and other on-line services.
- All software including purchased or licensed business software applications, municipality's-written applications, employee applications, computer operating systems, firmware, and any other software residing on municipality-owned equipment.
- All intellectual property and other data stored on municipality equipment.
- All of the above are included whether they are owned or leased by the municipality or are under the municipality's possession, custody, or control.

4 LEGISLATIVE FRAMEWORK

- Municipal Corporate Governance of ICT policy framework
- Protection of Personal Information Act
- Municipal Finance Management Act
- Cobit5
- ITIL
- King IV report

5 DISCIPLINARY ACTION

Compliance to this policy is mandatory. Negligence or misconduct could result in disciplinary procedures being instigated.

6 ICT RISK MANAGEMENT

Introduction

Risk is an event or cause leading to uncertainty in the outcome of ICT operations.

Related policy

This policy must be read with the municipality’s risk management policy.

Policy statement (s)

- ICT risks must be managed efficiently and effectively in accordance with ICT Governance framework policy.
- Risks must be identified and monitored periodically. ICT shall therefore provide assurance that risks are managed effectively.
- Users (councillors, employees and third-parties) must comply with council approved ICT risk and security policies and procedures.

7 ICT VENDOR AND SLA MANAGEMENT

Introduction

The delivery of ICT services to the municipality require specialist skills and varying capacity demands. The use of external service providers/vendors to provide ICT services can be a cost effective and reliable way of acquiring these skills at a reasonable cost and in the required timeframes. As a result, information security risks also extend across the supply chain and therefore service providers/vendors of ICT related services must be managed to ensure that these risks are controlled and mitigated where possible. ICT remains accountable for ICT services under the control of service providers/vendors.

Related policies

This policy must be read with Supply Chain Management and contracts management policies.

Policy statement (s)

- Service providers/ vendors appointed by the municipality must deliver the agreed services within the agreed times and cost.
- ICT contracts shall be stored centrally in the municipal archives.
- Service level agreements shall be signed for all vendors providing ICT services.
- Service provider’s performance shall be monitored periodically to ensure a high quality of service.

8 CHANGE CONTROL MANAGEMENT

Introduction

Ensuring effective change management within the municipality’s production ICT environment is extremely important in ensuring quality delivery of ICT services as well as achieving compliance. The intent of this policy is to ensure the effective management of change while reducing risk. ICT change management is the process of requesting, analysing, approving, developing, implementing, and reviewing a planned or unplanned change within the ICT infrastructure.

Policy statement (s)

- The change control process shall be formally defined and documented.
- All changes shall be effectively and efficiently managed.
- There shall be an approved quality assurance and a process in planning and implementing change.
- Changes shall be monitored periodically. The change management process begins with the creation of a change request within the municipality’s selected technology platform. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

9 ICT SECURITY MANAGEMENT

Introduction

Information security ensures that the municipality’s ICT systems, data and infrastructure are protected from risks such as destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data. The ICT systems manager is responsible for maintaining this policy.

This policy ensures the effective protection and proper usage of the computer systems and its peripherals within the municipality. The access to business applications, information systems, networks and computing devices within the ICT landscape must be managed and controlled.

All users (employees, consultants, contractors, third parties and temporaries) must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage municipal information assets. Information security requires participation and support from all information users.

Policy statement (s)

9.1 Securing workstations and hardware

- Equipment shall always be safeguarded appropriately - especially when left unattended.
- Only authorised personnel are permitted to take equipment belonging to the municipality off the premises
- Users shall be responsible for equipment’s security at all times when working off premises.

9.2 Managing network access controls

- Network resources shall be strictly controlled to prevent unauthorised access.
- Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.
- Connections to the network (including users' logon) shall be properly managed to ensure that only authorised devices / persons are connected.
- Unless authorized by the Accounting Officer, information may not be made available or disclosed to unauthorized individuals, entities or processes.

9.3 Controlling access to operating system software

- Access to operating system commands shall be restricted to those persons who are authorised to perform systems administration / management functions.
- Even then, such access must be operated under control requiring the specific approval of senior management.

9.4 Managing passwords/ pin codes

- Only authorised personnel shall create passwords
- Password shall expire in 30 days,
- Password complexity shall be activated
- Minimum password reuse shall be 5
- Remote password changes shall be managed

- Passwords shall not be shared with any other person for any reason.

9.5 Restricting Access

- Access controls shall be set out as per delegation and job description to minimise information security risks yet also allows the municipality's business activities to be carried without undue hindrance.
- Access must be created in such a way to comply with segregation of duties.

9.6 Giving Access to files and documents

- Access to information and documents shall be restricted to authorised.

9.7 Security controls

9.7.1 Physical Access

- Reasonable steps shall be taken to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery.
- ICT hardware under control of the ICT function shall be hosted in server rooms or lockable cabinets.
- Server rooms shall be of solid construction and locked at all times. Staff with authorization to enter such areas shall be provided with information on the potential security risks involved.
- Control access shall be restricted to authorised users.
- To reduce electrical circuits and forces beyond our control such as lightning and power surges, fire detection, suppression and environmental control systems shall be installed in the server room.
- These systems shall be monitored and maintained periodically.

9.7.2 Database security

- Full access to databases shall be limited to ICT staff who need this access.
- Officials who use applications shall not have these rights to the application's databases.

9.7.3 Network Security

Firewall management

- Firewall system shall be installed to monitor incoming and outgoing packet requests and to block any that may be from an untrustworthy source.

9.8 ICT security awareness

- ICT security awareness activities shall be undertaken to promote and maintain a positive security culture within and amongst the municipality’s ICT including contractors and third parties who have access to the systems.

9.9 Remote access and teleworking

- The application for remote access must be approved by the relevant head of department.
- Remote access sessions shall be effectively and efficiently managed.

9.10 ICT security aspects of business continuity management

- When business continuity plans are implemented, security risks shall be catered for.

9.11 Operating system security and administration

9.11.1 Appointing system administrators

- The municipality's systems shall be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems.

9.11.2 Administrating systems

- System administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the municipality, they shall be knowledgeable and conversant with the range of information security risks which need to be managed.

9.11.3 Managing operating systems and system administration

- The municipality's systems shall be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the municipality's information.

9.11.4 Managing system built accounts (administrator, root, guests)

- The above accounts should not be used regularly.
- Root and guest accounts must be disabled and must be used on accounting officer's approval.

9.11.5 Restriction of admin group

- The admin groups shall be controlled correctly and standard users must not access the local administrator accounts.

9.11.6 Managing system documentation

- System documentation is a requirement for all the municipality's information systems. Such documentation shall be kept up-to-date and be available.

9.12 Patch management

- ICT section shall identify patch management resources to update the servers and workstations of the municipality.
- Workstations shall have up-to-date operating system security patches installed to protect the asset from known vulnerabilities

10 USER ACCOUNT MANAGEMENT

Introduction

Information security is becoming increasingly important to the municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data. This policy ensures that the Municipality conforms to standard user access management controls.

Policy statement (s)

- User access management controls and procedures shall be developed in line with security policies and risks.
- The procedures shall include new user registration, terminated user removal, user permission/role change request, user access rights assignment, operating systems, databases /applications, reviewing user access permissions.
- Privileged user accounts shall be reviewed periodically

11 ICT ASSET MANAGEMENT

Introduction

This policy provides the overall framework for the management of ICT equipment from acquisition to disposal. The Municipality is committed to manage the lifecycle of its ICT assets and everyone has a duty to care and protect ICT assets at all-time whether they are in use, storage, movement or in disposal.

Related policies

This policy must be read with Asset Management, Asset Disposal, Records Management and Security policies

Policy statement (s)

11.1 Hardware Asset Management

11.1.1 Hardware Acquisition

- All computer hardware acquired by the municipality, including donations, shall be procured through the ICT office.
- Hardware shall not be connected, installed or operated within council property without authority of the ICT office.

11.1.2 Identification of equipment

- ICT assets shall be identifiable using a unique asset numbering system.

11.1.3 Disposing of obsolete equipment

- Equipment owned by the municipality shall only be disposed in line with municipal asset disposal policy.
- ICT shall ensure that the relevant security risks have been mitigated when ICT assets are disposed.

11.1.4 Hardware security

- To prevent the opportunist theft of unattended equipment all portable devices shall be stored, wherever possible, out of sight and preferably in a locked environment.

10.1.5 Hardware - stolen or damaged

- The user's line manager and ICT office shall be notified of any damage or theft of computer equipment.
- User must log a call with the ICT Helpdesk providing details of the incident.

11.1.5 Hardware - Change of user or relocation of equipment

- The ICT office shall be informed of all changes regarding relocation of computer equipment.
- All significant movement of ICT hardware shall involve the ICT and Assets offices.

11.1.6 Life cycle management of ICT equipment

- All ICT infrastructure's life cycle shall be managed effectively.

11.1.7 Insuring hardware

- All ICT equipment and other associated hardware belonging to the municipality shall carry appropriate insurance cover against hardware theft, damage, or loss.
- the equipment shall be replaced in terms of insurance cover in place, provided that such claims are not repudiated by the insurer concerned as being invalid on the basis that such loss or theft was occasioned by the negligence of the user concerned.

- Where the claim is found to be valid, municipality shall pay the excess on the claim.
- In instances where a claim is repudiated by the insurer as being invalid, the user shall be liable for costs of replacement.
- The user will further be responsible for reconnection and SIM swop charges irrespective of whether or not the claim is valid or not.

11.2 Software asset management

- Accurate inventory of assets shall be compiled.
- The municipality shall have the ability to provide proof of purchase for all software installed on their computer equipment.

11.2.1 Purchasing and installing software

- ICT section shall be informed timeously and be involved when the new software/ system is purchased.

11.2.2 Specifying user requirements for software

- All requests for new applications systems or software enhancements shall be presented to management committee with a business case and business requirements presented in a user software request form.

11.2.3 Disposing of software

- The disposal of software should only take place when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.

12 BUSINESS AND ICT CONTINUITY

Introduction

To ensure continuity of municipality’s operations, it is vital that there are reliable ICT operations that would ensure availability of supporting critical systems even under the most adverse circumstances.

Policy statement (s)

- Management shall ensure that ICT services continue in case of a disaster.
- Procedures and processes shall be in place to ensure effective and efficient ICT continuity.
- Each Head of Department shall perform a BIA in all processes to determine the criticality of these processes and to determine what the impacts are to the municipality if those processes were interrupted. He/she shall identify the process availability Recovery Time Objectives (RTOs), process Recovery Point Objectives (RPOs) and associated risks if these processes were not available.

13 DATA BACKUP AND RESTORE

Introduction

The ICT section is responsible for the backing up user data stored on the network servers, operating system images, systems application and critical content. The ICT section will have the primary responsibility of performing these functions on a daily basis. Monitoring of implementation and liaison with 3rd party providers will also be its responsibility.

Policy statement (s)

13.1 Data backup

- All municipality data shall be backed up.
- Backup data shall be stored at a location that is physically different from its original creation and usage location.
- Data restores shall be tested monthly.
- Procedures for backing up critical data and the testing of the procedures shall be documented.
- All data and software essential to the continued operation of the municipality shall be backed up.
- All supporting material required to process the information shall be backed up.
- Offsite storage site- Data backups shall be stored at least in two locations:

  a) on-site with current data in machine-readable format in the event that operating data is lost, damaged or corrupted; and

  b) One off-site to additionally provide protection against loss to the primary site and on-site data

- Off-site backups shall be a minimum of 20 kilometres from the on-site storage area in order to prevent a single destructive event from destroying all copies of the data.

13.2 Recovery of data backup

- Backup and recovery documentation shall be maintained, reviewed ad updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.

14 CAPACITY PLANNING AND AVAILABILITY MANAGEMENT

Introduction

Capacity management is the practice of planning, managing, and optimizing ICT infrastructure resource utilization. It balances cost vs. performance that requires insight into the current and future usage of computers, storage, and network resources. Capacity management determines how much capacity should be provided based on the information from demand management regarding what should be provided. In particular, capacity management is concerned with speed and efficiency.

Availability and capacity management allows ICT end-users to depend on the ICT services. If they rely on ICT to carry out activities, the ICT infrastructure must be reliable enough for this to happen whenever it is needed.

Policy statement (s)

- Adequate ICT capacity shall be available at all times to meet the agreed needs of the municipality in a cost-effective manner.
- The capacity management process shall work closely with service level management to ensure that the business requirements for capacity and performance can be met.
- Capacity management shall support the service desk and incident and problem management in the resolution of incidents and problems related to capacity.
- Infrastructure resource shall meet internal and external customer expectations for application performance and response.
- ICT service shall be available to end-users with as little disruption or downtime as possible.

15 INCIDENT AND PROBLEM MANAGEMENT POLICY MANAGEMENT

Introduction

Policy statement (s)

- All hardware faults should be reported promptly and recorded in a system.
- Incidents and weaknesses need to be reported at the earliest possible stage. This enables the ICT section to identify when a series of incidents or weaknesses have escalated to become a problem.

16 POLICY AMMENDMENT

This policy shall be reviewed and adopted by the council at least annually

17 PERMANENT / TEMPORAL WAIVER OF THE POLICY

- This policy may be partly or wholly waived or suspended by the municipal council on temporary or permanent basis.
- The Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to council.