

ICT Security Policy

2021/22

Summary

Publication Date	
Review Date	September 2021
Related Legislation/Applicable Section of Legislation	<ul style="list-style-type: none"> • Constitution of the Republic of South Africa Act, Act No. 108 of 1996. • Copyright Act, Act No. 98 of 1978. • Electronic Communications and Transactions Act, Act No. 25 of 2002 • Promotion of Access to Information Act, Act No. 2 of 2000. • Protection of Personal Information Act, Act No. 4 of 2013. • Regulation of Interception of Communications Act, Act No. 70 of 2002 • Municipal Finance Management Act, Act No. 56 of 2003. • Municipal Structures Act, Act No. 117 of 1998 • National Archives and Record Service of South Africa Act, Act No. 43 of 1996. • Local Government Municipal Systems Act No 32 of 2000 I.C.T. Good Practice and Standard

<p>Related Policies, Procedures, Guidelines, Standards, Frameworks</p>	<ul style="list-style-type: none"> • ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of ICT; it provides governance principles and a model. • The King III Code: The most commonly accepted Corporate Governance Framework in South Africa that talks to the establishment of I.C.T. Steering committee. • COBIT: Implementing Governance of ICT. • ICT Governance guidelines revised June 2012
<p>Replaces/ Repeals (whichever is relevant, if any)</p>	
<p>Policy Officer (Name/Position)</p>	<p>MW MXEKEZO</p>
<p>Policy Officer (Phone)</p>	<p>040-6733095</p>
<p>Policy Sponsor (Name/Position)</p>	
<p>Department Responsible</p>	<p>Corporate Services</p>
<p>Unit responsible</p>	<p>Information Communication Technology (ICT)</p>
<p>Applies to</p>	<p>Employees, Councillors and Vendors</p>
<p>Key Words</p>	<p>ICT Security Policy</p>

Status	Reviewal
Council approval date	
Version	1

REVISION RECORD

Date	Version	Revision Description

CONTENTS

1. TITLE 7

2. PURPOSE..... 7

3. SCOPE 7

4. PROCEDURE DETAIL..... 7-15

5. ROLES AND RESPONSIBILITIES..... 15-16

6. MONITORING, EVALUATION AND REVIEW16

7. DEFINITIONS AND ABBREVIATIONS..... 16-17

8. SUPPORTING DOCUMENTS.....17

9. REFERENCES17

10. APPENDIX.....17

1. TITLE

ICT Security Policy

2. PURPOSE

- The purpose of this policy is to ensure the Confidentiality, Integrity and availability of Information;
- To establish safeguards to protect the information resources from theft, abuse, misuse and any form of damage.
- To establish responsibility and accountability for Information Security in the Municipality.

3. SCOPE

This policy applies to all Ngqushwa Local Municipality employees and vendors appointed by the municipality. It is the responsibility of all 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, telecom equipment, networks, databases, printers, servers, shared computers, and all networks hardware.
- This policy addresses all risks associated to Information systems.

4. PROCEDURE DETAIL

4.1 PRINCIPLES

- The municipality perceives the significance of successful communication both inside the organization and remotely with its stakeholders.

- Only users and/or any other person specifically authorized by the Municipal Manager shall use the computing facilities provided by the NGQUSHWA LOCAL MUNICIPALITY.

4.2 POLICY PROVISIONS

- Users are responsible for maintaining the security of their own IT System accounts and passwords.
- A procedure of providing users who have forgotten their passwords with a new password shall be in place.
- Mandate processes to minimise risks associated with a disruption, disaster or failure of ICT systems.

4.3 CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

4.3.1 Securing unattended workstations

Equipment must always be safeguarded appropriately - especially when left unattended. Computer equipment, which is logged on and unattended can present a tempting target for unscrupulous staff or third parties on the premises.

4.3.2 Managing network access controls

ICT manager must ensure that access to the resources on the network must 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) have to 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.

4.3.3 Restricting Access

Access controls are to be set at an appropriate level, which minimises information security risks yet also allows the municipality's business activities to be carried without unnecessary interference.

4.3.4 Giving Access to files and documents

Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to sensitive information

4.4 SECURITY CONTROLS

4.4.1 Physical Access

- Servers shall be located in a secure server room that shall be accessed only by authorised ICT officials.
- Server rooms must be of solid structure and locked at all times.
- Third parties and contractors shall not access server room without any escort from ICT section.

4.4.2 Database security

- Full access to databases/System administration will be limited to ICT staff.
- Officials who use applications may not have these full rights to the application's databases

4.4.3 Network Security

a) Firewall Management

- Firewall is a network security system that must be installed to monitor and control incoming and outgoing network traffic based on predetermined security rules.
- Firewall provides barrier between a trusted internal network and untrusted external network, such as the Internet.
- Firewalls shall be installed within production environments where confidential information is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.
- Firewall Rules and Configurations require periodic review to ensure they afford the required levels of protection.
- Access to the Firewall is governed by password authentication.
- Only the ICT Manager and the Network Administrator are permitted access to the Firewall. Any changes to the device must be performed by either of the ICT Manager or the Network Administrator roles

b) Antivirus and Patch Management

- Anti-virus and patching are an important security mechanism required in the protection of computers in the municipality.
- The municipality's computers and servers must have supported anti-virus software installed on them.
- The anti-virus software must be scheduled to run at least once a day.
- The anti-virus software and virus pattern files must be up to date
- Virus infected computers must be removed from the network until they are confirmed as virus free
- Flash disks/ memory sticks are prohibited

- Any activities intended to create and/or distribute malicious programs into municipality's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

4.5 USER ACCESS MANAGEMENT

4.5.1 Access Control

- The allocation of access rights to users shall be strictly controlled through user access management controls and procedures, in terms of new user registration, terminated user removal, user permission/role change request, user access rights assignment on operating systems and databases /applications and reviewing user access permissions.
- Access to operating system commands is to 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 approvals of senior management.

4.5.2 Password

- Passwords shall be utilized to protect the confidentiality and integrity of municipal systems.
- when a password is initially assigned to a user the password shall be a temporary one and the user shall be forced to change it immediately;
- passwords shall be changed at least every 30 days;
- Users must avoid using guessable passwords such as 12345, abcdef, personal details.
- Password length must be at least eight (8) characters and be alphanumeric.

- Passwords shall not be shared by users, users who access other user's resource without authorization from ICT section shall be classified as an ICT security breach.

4.5.3 ICT Vendor access

- Access to municipal system without authorisation is prohibited.
- Vendors must be monitored at all-time when working on municipal systems.
- The vendor must sign ICT policy compliance form before accessing the systems.

4.6 DATA BACKUP AND RECOVERY

4.6.1 Data backup standards

Critical data, which is critical to the municipality, must be defined by the municipality and must be backed up. Backup data must be stored at a location that is physically different from its original creation and usage location. Data restores must be tested monthly. Procedures for backing up critical data and the testing of the procedures must be documented. These procedures must include, as a minimum, for each type of data:

- a) A definition of the specific data to be backed up;
- b) The type(s) of backup to be used (e.g. full back up, incremental backup, etc.);
- c) The frequency and time of data backup;
- d) The number of generations of backed up data that are to be maintained (both on site and off site);
- e) Responsibility for data backup;
- f) The storage site(s) for the backups;
- g) The storage media to be used
- h) Any requirements concerning the data backup archives;

- l) Transport modes; and
- j) Recovery of backed up data.

4.6.2 Data backup selection

All data and software essential to the continued operation of the municipality, as well as all data that must be maintained for legislative purposes, must be backed up. All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software. The application owner, together with the ICT Manager, will determine what information must be backed up, in what form, and how often (by application of the backup types template).

4.6.3 Backup types

Full backups should be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site. This statement will need to be reviewed once the ICT DR Business Impact and Risk Analysis requirements are updated with input from line managers and municipal operations.

Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.

In the event that a system requires a high degree of skill to recover from backup, consider taking full images of the servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.

4.6.4 Recovery of data backup

ICT Manager must make sure that backup and recovery documentation is maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:

- a) identification of critical data and programs and
- b) Documentation and support items necessary to perform essential tasks during a recovery process.

Documentation of the restoration process must include:

- a) Procedures for the recovery
- b) Provision for key management should the data be encrypted.

4.7 DELEGATIONS

Officials implementing this policy are required to refer to the latest delegation framework and identify the appropriate delegations applicable to this policy, which may be subject to change from time to time.

4.8 WAIVING OF THE POLICY AND IMPLEMENTATION PROVISIONS

Violation or non-compliance with this policy will give a just cause for disciplinary steps to be taken.

It will be the responsibility of Municipal Manager to enforce compliance with this policy.

4.9 COMMUNICATION

Circulars, messages and notices on notice boards will be utilized in order to inform all employees of the availability of the policy. Copies of the policy will also be distributed to the parties that took part in the consultation process

4.10 REVIEWAL OF THE POLICY

It will be the responsibility of the Corporate Services Department to consider the provisions of this policy on annual basis. The Corporate Services Department shall request all Departments to submit their proposed changes for submission to Council for approval.

5. ROLES AND RESPONSIBILITIES

Role	Authority
<p>Create, evaluate, review and adopt the Telephone, Cell phone & Data Card Policy</p>	<p>Council</p>
<ul style="list-style-type: none"> • Implement and enforce this policy • Establish and control the administration necessary to fulfil this policy, and report efficiently and regularly to the Committee in this regard. 	<p>Municipal Manager</p>

<ul style="list-style-type: none"> • Ensure that there is compliance with the Telephone, Cell phone & Data Card Policy 	<p style="text-align: center;">Director Corporate Services</p>

6. MONITORING, EVALUATION AND REVIEW

A report detailing the progress with the Implementation of Telephone, Cell phone & Data Card Policy with specific reference to achievement of this policy has to be compiled every year by the person with the responsibility for implementation and monitoring. The policy must be made available to all consulting parties for perusal and comment and must be circulated to all staff members by means of circulars, notices and notice boards.

7. DEFINITIONS AND ABBREVIATIONS

Term	Meaning
Alphanumeric	Password consisting of or using, letters, Special characters and numerals.
Antivirus	Designed to detect and destroy computer viruses.
Employees	Full official who are appointed permanent and on fixed term contract.
User	An Individual utilising Information Systems to achieve the business goals required to realise the mandate.

System	An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective
BIA	Business Impact Assessment

8. SUPPORTING DOCUMENTS

None

9. REFERENCES

None

10. APPENDIX

None

11. ADOPTION AND APPROVAL OF THE POLICY BY COUNCIL


This policy is adopted and approved by the full Ngqushwa Local Municipality Council for implementation



MUNICIPAL MANAGER

22/08/2022

DATE



MAYOR

30/08/2022

DATE