NGQUSHWA
MUNICIPALITY

Revised 2016-2017 Information and Communication Technology Policies

First adoption : 29 August 2012 at Council Chamber

Second adoption : 27 May 2013 at Mpekweni Beach Resort

Third adoption : 30 July 2015 at Council Chamber

Forth adoption : 7 March 2017 at Council Chamber

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.
- The **King III Code:** The most commonly accepted Corporate Governance Framework in South Africa that talks to ICT governance and establishment of I.C.T. Steering committee.
- **COBIT- Control objectives for Information and related technologies:** An internationally accepted process framework for implementing Governance of ICT.
- **UPS: Uninterruptible Power System:** is a surge protector that contains a high capacity rechargeable battery.
- **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.
- **Modem:** Electronic device that allows computers to communicate over telephone wires or cable-TV cable
- **BIA:** Business Impact Assessment.
- **PC:** Personal computer

Enabling Legislation

- 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.
- Minimum Information Security Standards, as approved by Cabinet in 1996.
- Municipal Finance Management Act, Act No. 56 of 2003.
- Municipal Structures Act, Act No. 117 of 1998.
- Municipal Systems Act, Act No. 32, of 2000.
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
- 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.
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.
- Local Government Municipal Systems Act No 32 of 2000 I.C.T. Good Practice and Standard
- 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

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. In addition, clearly written ICT policy and procedures simplify compliance with ISO (International Standards Organization).

Scope of the policy

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, telecomm equipment, networks, databases, printers, servers, shared computers, and all networks hardware.

- 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.

1. SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

A. Hardware

1.1 Acquisition

1.1.1 Except for minor purchases, hardware shall be purchased through a structured evaluation process which shall include the development of a detailed request for proposal (RFP)/specification document.

1.1.2 The I.C.T. personnel shall verify and approve specifications for all-new electronic information equipment and software prior to purchase by each department.

1.1.3 New computer equipment shall be purchased and shall conform to the following minimum standard of quality and ability:
PC Specifications: Intel Core i7 2.3 GHz Processor, 500GB HDD, 8GB RAM, DVD Combo, VGA, gigabit LAN card, wireless and bluetooth. Win 10 Pro 64 bit, carry case, security cable and 3YR onsite warranty.
Other than the above specifications the Accounting officer must approve.

1.1.4 The life span of a desktop and laptop PCs is 3 years.

1.2 Installing new Hardware

All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date.

1.3 Supplying Continuous Power to Critical Equipment

An Uninterruptible Power Supply (UPS) is to be installed to ensure the continuity of services during power outages. If the mains power fails for any reason, the system will crash and data files may be corrupted.

1.4 Using fax machines / fax modem

Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible. Both the owner of the information and the intended recipient must authorise the transmissions beforehand.

1.5 Using centralised, networked or stand-alone printer

Information classified as highly confidential or top secret, may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing.

1.6 Issuing stand-alone printers

Local printer are to be issued to all heads of departments and middle managers. Usage is restricted to business purposes.

1.7 Installing and maintaining network cabling

Network cabling should be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall mounted sockets. Any unused network wall sockets should be sealed-off and their status formally noted.

B. Consumables

1.1 Controlling ICT consumables

ICT consumables must be purchased in accordance with the municipality's approved purchasing procedures with usage monitored to discourage theft and improper use e.g. toners, cartridges, ribbons etc.

1.2 Using removable storage media including flash disks and CDs

Only personnel who are authorised to install or modify software shall use removable media to transfer data to and from the municipality's network. Any other persons shall require specific authorisation.

C. Working off premises

1.1 Issuing laptop / portable computers to personnel

Laptop PCs are to be issued to all computer users starting except for trainees and casual workers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices. Desktops will only be issued as requested by the line managers.

1.2 Using laptop/portable computers

Users who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.

1.3 Moving hardware from one location to another

Movement of hardware between the municipality's locations is to be strictly controlled by I.C.T. personnel.

D. Documenting hardware

Maintaining a hardware inventory or register

A formal hardware inventory of all equipment is to be maintained and kept up to date at all times.

E. Other hardware issues

1.1 Disposing of obsolete equipment

Equipment owned by the municipality may only be disposed by authorised personnel and ICT manager must ensure that the relevant security risks have been mitigated.

1.2 Recording and reporting hardware faults

All hardware faults are to be reported promptly and recorded in a hardware fault register.

1.3 Taking equipment off the premises

Only authorised personnel are permitted to take equipment belonging to the municipality off the premises; they are responsible for its security at all times.

1.4 Maintaining hardware (on-site or off-site support)

All equipment owned, leased or licensed by the municipality must be supported by appropriate maintenance facilities from qualified engineers

1.5 Damage to equipment

Deliberate or accidental damage to municipality property must be reported to the I.C.T. office as soon as it is noticed.

1.6 Insuring hardware

All ICT equipment and other associated hardware belonging to the municipality must carry appropriate insurance cover against hardware theft, damage, or loss."

1.7 Instances where I.C.T. equipment is stolen or lost:

1.7.1 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;

1.7.2 Where the claim is found to be valid, the user concerned shall be liable for the payment of the excess on the claim. A replacement equipment will only be handed over to the user, once the said excess has been paid.

1.7.3 In instances where a claim is repudiated by the insurer as being invalid, the user shall be liable for costs of replacement.

1.7.4 the user will further be responsible for reconnection and SIM swop charges irrespective of whether or not the claim is valid or NOT.

2. CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

2.1 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.

2.2 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.

2.3 Controlling access to operating system software

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 approval of senior management.

2.4 Managing passwords/ pin codes

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason.

2.5 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 undue hindrance.

2.6 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

2.7 Security controls

2.7.1.Physical Access

The ICT Manager must take reasonable steps 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 must be hosted in server rooms or lockable cabinets. Server rooms must 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.

2.7.2. Database security

The ICT Manager must limit full access to databases to ICT staff who need this access. Officials who use applications may not have these rights to the application's databases

2.7.3.Network Security

Firewall Management

ICT manager must ensure that firewall system is installed to monitor incoming and outgoing packet requests and to block any that may be from an untrustworthy source.

Information security requires the participation of and support from all information users. 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. Training and documentation with respect to information security is the responsibility of the ICT manager assisted by the Network Administrator.

Firewall planning and implementation should be addressed in a phased approach as follows:

1. **Plan.** The first phase of the process involves identifying all requirements that the Municipality should consider when determining which firewall to implement to enforce the Municipality's security policy.
2. **Configure**. The second phase involves all surfaces of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system.
3. **Test.** The next phase involves implementing and testing a prototype of the designed solution. The primary goals of testing are to evaluate the functionality, performance, scalability, and security of the solution, and to identify any issues.
4. **Deploy**. Once testing is completed and all issues are resolved, the next phase focuses on deployment of the firewall into the enterprise.
5. **Manage**. After the firewall has been deployed, it is managed throughout its lifecycle to include component maintenance and support for operational issues. This lifecycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

2.7.1.1 Roles and responsibilities

ROLE	FUNCTIONAL RESPONSIBILITIES
Council	• Council shall ensure that the necessary information security controls are implemented and complied with as per this policy.
Municipal Manager	• approval of changes on firewall systems • Approve and authorise changes made on firewall systems on behalf of the municipality.
Manager: ICT	• Document and disseminate information security policies, procedures, and guidelines • Coordinate the development and implementation of municipality's security training and awareness program. • Coordinate a response to actual or suspected breaches in the confidentiality, integrity or availability of information assets. • Inform users about security measures
Information	• Explain potential threats, install software,

Security Officer/ Network Administrator	implement security measures and monitor networks. • Recognizes problems by identifying abnormalities; reporting violations • Assist on configuration of firewall systems.

3. PROCESSING INFORMATION AND DOCUMENTS

3.1 Networks

3.1.1 Configuring networks

The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.

3.1.2 Managing the network

Suitably qualified staff must manage the municipality's network, and preserve its integrity in collaboration with the nominated individual system owners.

3.1.3 Accessing the network remotely

Remote access to the municipality's network and resources will only be permitted providing that authorised users are authenticated, data is encrypted across the network, and privileges are restricted.

3.1.4 Defending the network information from malicious attack

System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.

All known vulnerabilities – in addition to all suspected or known violations – must be reported in an expeditious and confidential manner to the ICT office immediately.

3.2 Operating system security and administration

3.2.1 Appointing system administrators

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

3.2.2 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 must be knowledgeable and conversant with the range of information security risks which need to be managed.

3.2.3 Managing operating systems and system administration

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

3.2.4 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.

3.2.5 Restriction of admin group

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

3.2.6 Managing System Documentation

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

3.2.7 Change Control Management

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical municipality's information resources (such as hardware, software, system documentation and operating procedures).

3.3 Email and World Wide Web

3.3.1 Internet

Internet shall be used as another delivery channel to offer communication and information to users.

3.3.2 Intranet

Intranet is devoted to municipality's departments and/or business units to make internal communication more efficient and effective.

3.3.3 Extranet

Extranet, or extended internet, shall be used by the municipality to form a tight electronic communications channel relationship with its government structures or the private sector in the case of e procurement and e-governance.

3.3.4 Email

Municipality's supplied e - mail service is to make both external and internal work related communication more efficient and effective. Both internal and externally based browser e-mail shall, if accessed by using Ngqushwa Local Municipality's infrastructure and supplied internet channels, be deemed to be governed by this policy.

3.4 Downloading files and information from the internet

Care must be taken when downloading information and files from the internet to safeguard against both malicious code and also inappropriate material.

3.5 Unacceptable uses of the internet and e – mail

The municipality's e-mail and internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or

Xrated. Sending of racially or sexually harassing message/files is also prohibited. No abusive, profane or offensive language is to be transmitted through the municipality's e mail or internet system.

Electronic media may not be used for any other purpose that is illegal. Solicitation of non Ngqushwa Local Municipality business or any use of Ngqushwa Local Municipality e mail or internet for personal gain is prohibited. The use of e-mail to participate in political activities, solicit political support or propagate political views is prohibited.

Copyrighted material belonging to entities other than Ngqushwa Local Municipality, may not be transmitted by employees on Ngqushwa Local Municipality's e – mail /internet system. All employees obtaining access to other than companies' or individuals' materials must respect all copyrights and may not copy, retrieve or forward copyrighted holder, or as a single copy for reference/back up purposes only.

3.6 Virus scan of E – mail

All inbound and outbound electronic mail must be scanned for viruses before delivery. The scanning should include attachments zipped or otherwise. The exception would be encrypted e-mail. Specific policies relating to encrypted mail apply in this case.

3.7 Developing a web site

Due to the significant risk of malicious intrusion from unauthorised external persons, web sites may only be developed and maintained by properly qualified and authorised personnel.

3.8 Using internet for work purposes

Management is responsible for controlling user access to the internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of information security incidents.

3.9 Maintaining the web site

The web site is an important marketing and information resource for the municipality, and its safety from unauthorised intrusion is a top priority. Only qualified authorised persons may amend the web site with all changes being documented and reviewed.

3.10 Data management

3.10.1 Using meaningful file names

The naming of the municipality's data files must be meaningful and capable of being recognized by its intended users.

3.11 Document handling

3.11.1 Photocopying confidential information

All employees to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as highly confidential or above.

3.12 Securing data

3.12.1 Fire Risks to the information

All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded

To reduce electrical circuits and forces beyond our control such as lightning and power surges, fire detection system and suppression systems must be installed in the server room.

3.12.2 Floods

To provide a degree of hardware protection in case of flooding raised floor at server room must be used.
And also to run cabling between devices under the floor, minimizing trip hazards and the possibility of accidental disconnects.

3.12.3 Dealing with sensitive financial information

Sensitive financial information is to be classified as highly confidential and must be afforded security measures which, in combination, safeguard such information from authorised access and disclosure.

3.12.4 Deleting data created /owned by others

Data is to be protected against unauthorised or accidental changes, and may only be deleted with the proper authority.

3.12.5 Protecting Documents with Passwords

Sensitive / confidential electronic data and information should be secured, whenever possible, with access control applied to the directory on the (computer) system concerned. The sole use of passwords to secure individual documents is less effective, and hence discouraged, as passwords may be either forgotten or become revealed (over time) to unauthorised persons.

3.13 Other information handling and processing

3.13.1 Loading personal screen savers

Employees are not permitted to load non-approved screen savers onto the municipality's PCs i.e. laptops and workstations.

3.13.2 Playing games on office computers

The playing of games on office PCs is prohibited.

3.13.3 Using photocopier for personal use

The use of photocopiers or duplicators for personal use is discouraged. In exceptions, specific permission must be given by the employee's immediate supervisor or manager.

3.13.4 Travelling on Business

Employees travelling on business are responsible for the security of information in their custody.

4. TELECOMMUNICATIONS

4.1 Provision of telephone service

4.1.1 It is the responsibility of the municipality to provide all the municipal offices with the satisfactory and reliable telephone services. The telephone operating system must be centralized through which all outgoing and incoming calls shall be routed;

4.1.2 The municipal switchboard and the switchboard instrument as well as the office in which the switchboard is housed shall be provided with a lockable device/s, the keys of which shall be in the possession of the receptionist.

4.1.3 It is the responsibility of the receptionist to ensure that no unauthorized person obtains access to the switchboard.

4.2 Telephone usage control measures

4.2.1 The use of the municipality's telephone will be monitored for inappropriate call patterns, unexpected costs, and excessive personal use.

4.2.2 Each staff member shall sign an understanding that if they make private calls, the cost thereof shall be deducted from their salaries.

4.2.3 The Accounting Officer must determine which officials may have private lines to their offices for use in connection with the performance of their duties;

4.2.4 Where an employee has a direct dialing facility, that employee shall be obliged to maintain the telephone log book and submit it to the I.C.T. section at the end of the month.

4.2.5 No officials will be entitled to make international calls unless approved by the Accounting Officer

4.3 Control procedures

Every Executive Manager/Manager must personally examine telecommunication accounts relating to lines or extensions allocated to employees under his/her supervision. He or she shall make such relevant comments for attention or information of the relevant person, his or her supervisor, or any other official in the department, which shall where necessary be used as evidence should a disciplinary hearing or such appropriate actions be necessary to be taken due to persistent abuse by an employee.

4.4 Telephone accounts

4.4.1 The ICT section will issue out telephone statements of account for each official on request.

4.4.2 Telephone statements will be delivered to the line managers, who will inspect such statements before distributing them to the respective employees.

5. CELLULAR PHONES AND DATA CARDS/ MODEMS

5.1 Gazette on determination of upper limits, allowances and benefits for councilors requires that the municipality must give councillors cellphone allowance and mobile data allowance therefore, municipality enters into a contract with a cellular service provider on behalf of councilors and assign cellular contracts accordingly.

5.2 HODs and middle management are automatically allocated 3G modems.

5.3 Drivers, traffic officers and supervisors are automatically allocated cellular phone contracts to an amount not exceeding R 350.00 monthly

5.4 Municipal Manager is automatically allocated cellular phone contract to an amount not exceeding R 1500 monthly.

5.5 Executive Managers are automatically allocated cellular phone contracts to an amount not exceeding R 1300.00 monthly

5.6 For other employment levels, each application will be considered on its own merit, irrespective of the rank of the applicant for approval by the HOD and Accounting Officer. The nature of the work and the need for a 3G card and as a means of carrying out the job are to be the determining factors.

5.7 In support of an employee's application for a 3G card. Fully motivated proof must be submitted to the relevant HOD, to the effect that availing a 3G card is the most economical and practical instrument of accessing e-mails and internet, and that it will enhance the official's work performance.

5.8 Any exceptions to the eligibility criteria or any other aspects of this policy will be at the Municipal Manager's discretion, documented and requested by line Head of Department.

5.9 Cellphone and 3G card usage agreement will be signed by both user and municipality as the control measure.

6. PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE

Ngqushwa Local Municipality prefers Microsoft platform.

6.1 Software

6.1.1 Purchasing and installing software

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

6.1.2 Specifying user requirements for software

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

The following is a list of fully supported, standard software that is installed on municipal owned end-user devices.

- Microsoft windows professional edition
- Microsoft office standard and professional editions

Other supported software titles, available upon request, include:

- Microsoft project
- Microsoft visio
- Sage Evolution
- VIP HR and Payroll system
- Caseware and any other that is approved by the Accounting officer

Installation of software listed below is expressly forbidden:

- Privately owned software
- Internet downloads

- Pirated copies of any software titles
- Any software not installed according to the procedures set out in this policy

6.1.3 Selecting office software packages

All office software packages must be compatible with the municipality's preferred and approved computer operating system and platform.

6.1.4 Using licensed software

To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements are to be strictly adhered to.

6.1.5 Implementing new / upgraded software

The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased information security risks associated with such projects are mitigated using a combination of procedural and technical control techniques.

Software must be installed on municipal owned end-user devices by ICT staff members after approval from the Municipal Manager.

All software installed on municipal systems must be used in compliance with all applicable licenses, notices, contracts, and agreements.

ICT unit reserves the right to uninstall any unapproved software from a municipal owned machine. No municipal software is to be installed on privately owned computers as this is against Code of Conduct for Municipal Staff Members (Schedule 2, No 9 (Council Property)) as stipulated in the Municipal Systems, No 32 of 2000.

6.2 Other software issues

6.2.1 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.

6.2.2 Training in new systems

Training is to be provided to users and technical staff in the functionality and operations of all new systems.

6.2.3 Documenting new and enhanced systems

ICT staff must be involved when new and enhanced systems are acquired and must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

7. VIRUS HANDLING AND PATCH MANAGEMENT

Anti-virus and patching are an important security mechanism required in the protection of computers in the municipality.

7.1 .The municipality's computers and servers must have supported anti-virus software installed on them.

7.2 . The anti-virus software must be scheduled to run at least once a day.

7.3 .The anti-virus software and virus pattern files must be up to date

7.4 .Virus infected computers must be removed from the network until they are confirmed as virus free

7.5 .Flash disks/ memory sticks are prohibited

7.6 .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.

8. DATA BACKUP AND RECOVERY

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. 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. ICT Manager is responsible for maintaining this policy.

Each Head of Department must 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

8.1 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;
i) Transport modes; and
j) Recovery of backed up data.

8.2 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.

8.3 Backup types

8.3.1 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.

8.3.2 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.

8.3.3 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.

8.4 Recovery of data backup

ICT Manager must make sure that backup and recovery documentation is maintained, reviewed ad 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.

9. ICT SLA MANAGEMENT

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. It is for this reason that the management of service providers/vendors is an important Municipal task to ensure that service providers/vendors deliver the agreed services within the agreed timeframes and cost. ICT Manager is responsible for managing the SLAs and all ICT contracts must be stored centrally in the municipal archive.

9.1 The following terms and conditions must be defined in all ICT service provider/vendor contracts:

a) A description of the ICT services and how they will be delivered;
b) The monthly fees and deliverables attached to the fees;
c) The cost structure and payment schedule;
d) The period of the contract, renewal and termination clauses;
e) Availability, reliability and capacity of person/s responsible for delivering the service;
f) Confidentiality and non-disclosure;
g) In the case of software development:
    a. Who owns the program as well as the ideas and processes that makes it a valuable piece of software within the Municipal environment;
    b. 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;
    c. Who is responsible for, and how, the software will be maintained in the future;
h) Which data the service provider/vendor may have access to, who owns the data, and how the data must be protected in line with the ICT Security Controls Policy;
i) The responsibilities of both parties for ICT disaster recovery;
j) Municipality's involvement in service provider/vendor processes, as well as the right to send its own audit team;
k) Service Provider/Vendor service reporting;
l) How the service provider/vendor will ensure that the resources/skills are available for the duration of the agreement;

m) Skills transfer to the municipality;
n) Monitoring of critical systems in real-time and providing appropriate alerts to the ICT Manager.
o) The security requirements of the person(s) delivering the ICT service in line with the ICT Security Controls Policy as well as the ICT Operating System Security Controls Policy;
p) Should the service provider/vendor store or process personal information on behalf of the Municipality, the contract must state that the information must be protected in line with the ICT Security Controls Policy.
q) Restrictions on the use of sub-contractors;
r) In the event of a security breach affecting personal information, the service provider/vendor must notify the Municipality immediately;
s) Penalties or discounts for non-performance against service levels;
t) The process to terminate the agreement, without disrupting the ICT service to the municipality; and
u) Monthly report and meetings where applicable

9.2 The ICT Manager must ensure that service providers/vendors produce reports that include, but not limited to, the following information:
a) Service level performance statistics, with failures and consequences;
b) Major events;
c) Incidents logged and resolution;
d) Capacity usage and growth trends;
e) Change requests and status; and
f) Details of charges and invoices.

9.3 The agreement with the service provider/vendor must indicate the response time from the service provider/vendor based on the level of impact. The table below contains an example:

Impact	**Description**	**Service level**
Priority 1 Very high	The whole Municipality affected Extensive financial impact	12 hours
Priority 2 High	More than half of Municipality affected Single department affected Significant financial impact	24 hours
Priority 3 Medium	Single user affected by an incident Limited financial impact	48 hours
Priority 4 Low	Enhancement or new capability Service request from a user	To agreed timelines

9.4 The ICT steering committee must nominate the ICT Manager as the service manager for each ICT contract. The ICT steering committee may nominate any other municipal employee to manage the service of

ICT-related contracts if the contract is outside of the ICT Manager's scope of responsibility e.g. a financial or human resources system.

9.5 The ICT Manager must ensure that the services received from service providers/vendors are dependent on contact meetings and performance reviews. The amount of time and effort spent managing service providers/vendors must be equal to their importance to the Municipality.

10. USER ACCESS MANAGEMENT

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. ICT Manager must develop user access management controls and procedures in terms of new user registration, terminated user removal, user permission/role change request, user access rights assignment, operating systems, databases /applications and reviewing user access permissions

11. COMMENCEMENT

This policy will come into effect on the date of adoption by Council.

12. COMPLIANCE AND ENFORCEMENT

Violation or non-compliance with this policy will give a just cause for disciplinary steps to be taken.
It will be the responsibility of Council to enforce compliance with this policy.

13. POLICY AMENDMENT

This policy will be reviewed by ICT manager and be adopted by council at least annually.

Recommended by: ..... 7 May 2017

Mr. T.T. Mnyimba Date

Municipal Manager

Approved by: ..... 7 May 2017

Cllr. M. Siwisa Date

Mayor