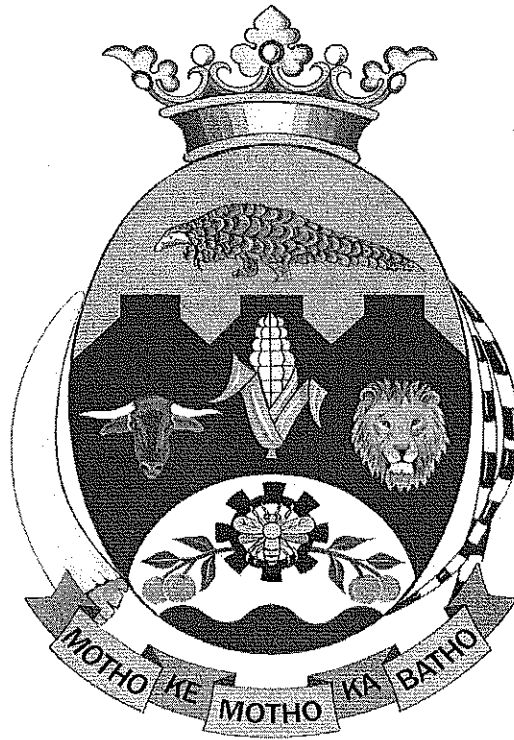


LEPELLE-NKUMPI MUNICIPALITY



INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICY

This policy contains 38 pages
ICT Security policy - Lepelle-Nkumpi

A handwritten signature in black ink, located in the bottom right corner of the page.

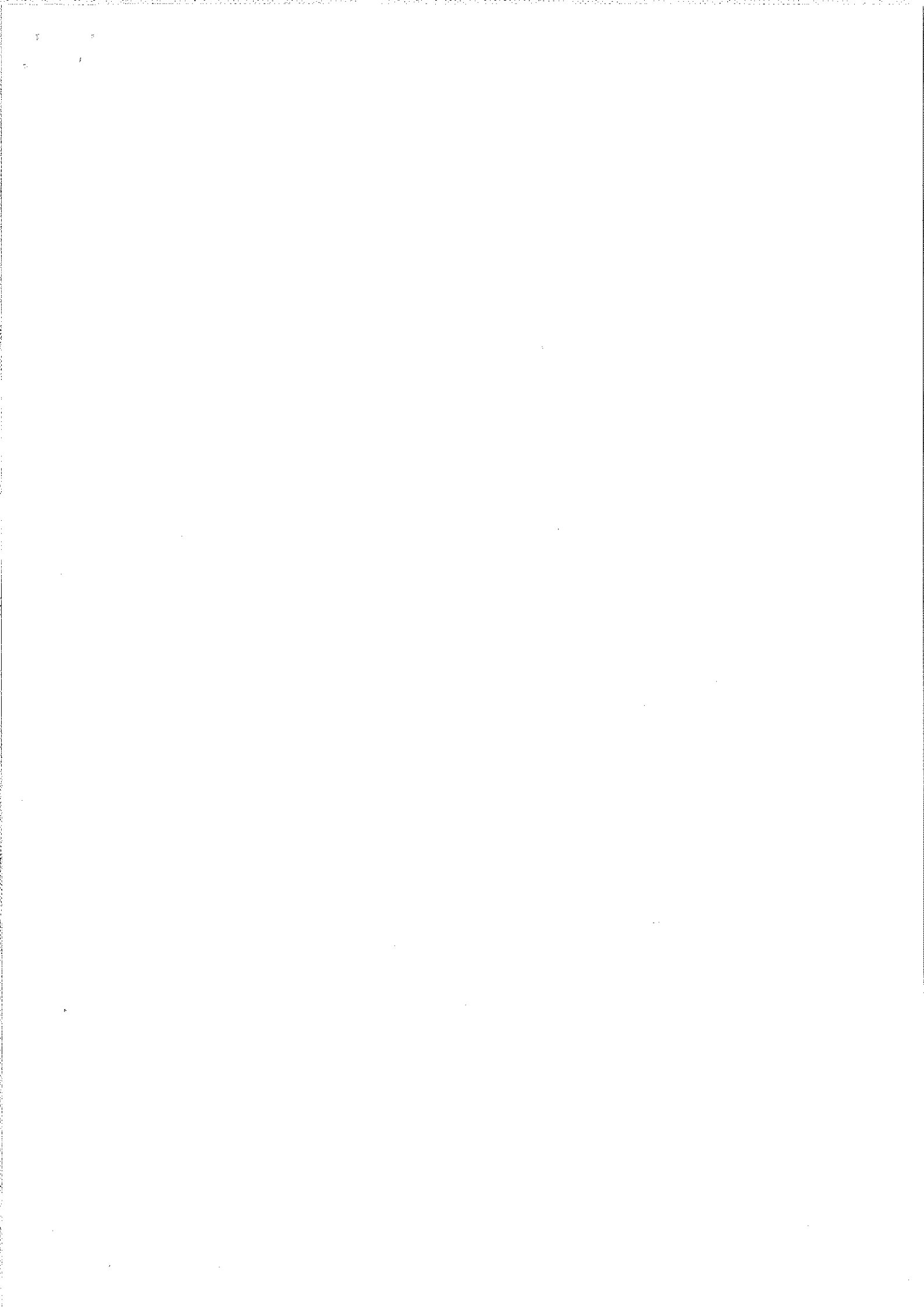
Contents

2.	Objectives and scope	5
2.1	Objectives	5
2.2	Scope	5
2.3	References	5
2.4	Policy statement	6
2.5	Non-compliance	6
3.	Accountability for assets	7
3.1	Objective	7
3.2	Policy statement	7
3.3	Requirements	7-8
4	Personnel responsibility for security incident reporting	9
4.1	Objective	9
4.2	Policy Statement	9
4.3	Reporting and evaluation of security incidents and weaknesses.	9
4.4	Actions and follow up	9-10
5	Physical and environmental security	11
5.1	Objective	11
5.2	Policy statement	11
5.3	Security standards for ICT rooms	11
5.3.1	Space and layout	11
5.3.2	Work practices	11
5.3.3	Security	12
5.3.4	Power	12
5.3.5	Fire	12
5.3.6	Air Conditioning	13
5.3.7	Environmental control and monitoring	13
5.3.8	Lighting	13
5.3.9	Cleaning	13
5.4	Security access to ICT rooms	13
5.4.1	Rules for Executive Managers, Managers and Staff members	14
5.5	Security of Removable Media	15
5.5.1	Backup Media	15
5.5.2	Media in transit	15
5.5.3	Archives	15
5.5.4	Identification of media	15

5.5.5	Recovery of data	16
5.5.6	Electronic media disposal	16
6.	System access control	17
6.1	Objective	17
6.2	Policy statement	17
6.2.1	Security requirements for ICT projects	17
6.2.2	User & access rights	18
6.2.3	Password, user ID and access rights administration	18-19
6.2.4	Security monitoring	19
7.	System development and maintenance	21
7.1	Objective	21
7.2	Policy statement	21
7.3	Initiation and approval of a change or development project	21
7.4	Product development	21
7.5	Requirements analysis	22
7.6	Development approach	22
7.7	Module testing	22
7.8	System testing	22
7.9	Acceptance testing	22
7.10	Release planning	23
8.	End user computing policy	24
8.1	Objectives	24
8.2	Policy statement	24
8.3	Internet use	24
8.3.1	Internet usage standards	24
8.3.2	Anti-virus measures	25
8.3.3	Monitoring of Internet use	25
8.3.4	Internet security awareness	25
8.3.5	Additional connections to the Internet	26
8.3.6	Who qualifies for 3G Cards	26
8.3.7	Internet Security Policy Statements	26-28
8.3.8	Non-Compliance	28
8.4	Use of Electronic Mail Facilities	28
8.4.1	General Requirements	29
8.4.2	E-Mail Disclaimer	30
8.4.3	Attachments to e-mail Messages.	30
8.4.4	Size of the user's mailbox	30
8.4.5	Non-compliance	31

8.5	Anti-Virus Security	31
8.5.1	Policy Statement	31
8.5.2	Requirements	32
8.5.3	Enforcement	32
8.6	Use of computer hardware and software	32
8.6.1	Acquisition and allocation of Computer Equipments	32
8.6.2	Management of ICT Equipments	33
8.6.3	Standardization of ICT Equipments	33
8.6.4	Non-standard items will not be supported	34
8.6.5	Allocation of personal computers as well as laptops to employees	34
8.6.6	Classification of Computer Users	34
8.6.7	Use of Computer equipment for official purposes	35
8.6.8	Use of Computer equipments for non-official purposes	35
8.6.9	Storing of material on computer equipment	35
9.	Laptop /Notebook Policy	36-37
10.	Printers	37
11.	Executive Manager's Responsibility	37
12.	Don'ts and Do's	38





2. Objectives and Scope

2.1 Objectives

This document states the policy of Lepelle-Nkumpi Municipality for the application of ICT security disciplines to protect its data, systems and applications against all threats, which could endanger their confidentiality, integrity and availability.

2.2. Scope

This policy applies to all users of applications and the ICT systems within Lepelle-Nkumpi Municipality. It applies across hardware platforms, to all business units and to all Executive Managers, Managers, staff and contractors of Lepelle-Nkumpi Municipality.

This policy is mandatory for all offices of Lepelle-Nkumpi including satellite offices where the Lepelle-Nkumpi computer system has been installed. All Executive Managers, Managers, staff members and contractors will be required to sign a statement on a yearly basis acknowledging their understanding of, and compliance with the policy.

2.3. References

This policy document shall be read in conjunction with the following Acts and Standards:-

- The Constitution of the RSA, Act 108 of 1996
- Municipal Finance Management Act 1 of 2004
- Local Government Municipal Structures Act 117 of 1998
- Local Government Municipal Systems Act 32 of 2000
- Minimum Information Security Standards (MISS)
- State Information Technology Agency (SITA) Act, as amended
- Electronic Communication Transaction Act
- The Protection of Access to Information Act 84 of 1982
- The Promotion of Access to Information Act
- Information Security Policy: Securing Information in the digital Age



- The National Archives Act 43 of 1996.

2.3. Policy statement

Computer system resources and associated data are business critical assets requiring a high level of protection. It is Lepelle-Nkumpi Municipality's policy that sufficient measures should be taken to protect these assets against accidental or unauthorized modification, disclosure or destruction, as well as to assure the confidentiality, integrity and availability of Lepelle-Nkumpi Municipality's automated data processing activities.

2.4. Non-compliance

Non-compliance with the standards and policies covered in this statement will be dealt with according to Human Resource policies.

Non-compliant end-users will face disciplinary hearings and disciplinary action taken against such my include dismissal.

Handwritten signature or initials in the bottom right corner of the page.

3. Accountability for assets

3.1. Objective

To maintain appropriate protection and management of ICT assets.

3.2. Policy statement

It is the responsibility of each Executive Manager, Manager, employee and contractor to ensure that the entire municipality's assets or assets used to access the municipality's ICT infrastructure are adequately accounted for. Information or changes in ownership, allocation of these assets, changes in configuration and usage outside of the Municipality's premises must be communicated to the ICT Manager.

In order to protect the municipality's assets adequately, identification should be made of all of assets for which the ICT Manager has security responsibility. All major ICT assets should be accounted for as accountability for assets helps ensure that adequate security protection is maintained. An inventory of assets must be maintained to ensure that effective security protection is implemented.

3.3. Requirements

Critical ICT assets should be identified and appropriately documented. Critical assets include:

- Network interconnection components (routers, switches, hubs and all IT related Equipments.)
- Servers (email, file, proxy, antivirus, e-Venus and all other servers.)
- External connection components (modems, remote access servers)
- Security components (authentication servers, firewalls)
- PC's and laptops.

Appropriate documentation concerning the municipality's critical ICT assets must be available and should cover:

- Identification: every critical ICT asset should be uniquely identified. The identification scheme used for this must ensure that:
 - The location of the ICT assets is known



- The supplier of the ICT asset is known (supplier information must be available)
- Maintenance contracts for the ICT assets are identified.
- Persons responsible for the assets are known.
- **Description:** a short description should be available for every critical ICT asset. The description should include general information on the critical ICT assets, such as its main function and use.
- **Configuration:** Information on its configuration should be available for every critical ICT assets. Technical configuration documentation should be included and supported by business requirements explaining why the ICT asset has been configured as such.
- **Linkages (where appropriate):** Information on links with other critical ICT assets should be included.

The ICT division should keep an ICT inventory register that should be updated with all additions to ICT assets. All critical ICT assets should be entered individually indicating the following:

- **Model and type** : the model and type of the ICT asset;
- **Serial number** : the serial number of the ICT asset;
- **Identification** : a unique identification number (where relevant);
- **Location** : the location of the ICT asset;
- **Supplier**: the supplier's name.

The above is mandatory for all critical ICT assets.



4. Personnel responsibility for security incident reporting

4.1. Objective

To ensure proper and timely reporting and subsequent resolution of all security incidents.

4.2. Policy Statement

Security incidents need to be identified, recorded, and escalated where appropriate and resolved. All Executive Managers, Managers and employees should be aware of and follow the procedure for reporting the different types of incidents (security breach, threat, weakness or malfunction) that might impact the security of the municipality's assets.

4.3. Reporting and evaluation of security incidents and weaknesses.

All security incidents should be reported according to the procedures as laid down and adjusted from time to time by the ICT division. Personnel should understand their responsibility for reporting security incidents as quickly as possible. A security incident is any incident which may affect or has affected:

- The confidentiality of the municipality's information (electronically stored)
- The integrity of the municipality's data
- The availability of the municipality's ICT systems

The IT division should evaluate and record all incidents reported. These incidents include:

- Virus incidents
- Resource/network attacks
- Operational Incidents
- Loss Incidents

4.4. Actions and follow up

Reporting of security incidents must result in specific countermeasures taken by the ICT Manager. Any action taken as a result of a security incident reported should at the minimum specify:

- What the action is

- Who will own the action
- When the action is expected to be resolved.

AA
RCA

5. Physical and environmental security

5.1. Objective

To prevent unauthorized access to, damage to, interference with and interruption of ICT services.

5.2. Policy statement

Executive Managers, Managers, and all employees should ensure that equipment containing municipal information is physically secured at all times.

ICT facilities supporting critical or sensitive municipal activities should be housed in secure areas. These areas should be accessible only by properly authorized individuals and protected from intentional and accidental damage. Data can be compromised through the careless disposal of equipment. All items of equipment containing storage media, including fixed hard disks, should be checked to ensure that any sensitive data and licensed software are removed or overwritten prior to disposal.

5.3. Security standards for ICT rooms

5.3.1. Space and layout

There must be sufficient physical space available for the equipment housed both current and planned. The equipment must be best located in terms of:

- operational functionality and use
- air circulation
- health and safety
- Maintenance access to the equipment.

Bulky and heavy equipment must be housed in floor standing cabinets.

5.3.2. Work practices

Everyone entering an ICT room must:

- be authorized
- maintain cleanliness of the room
- dispose of all rubbish



- refrain from eating or drinking within the room.

Staff responsible for maintaining the room must ensure that a copy of these practices is displayed in the room.

Cabling must be kept tidy and designed not to cause any work hazards. Cable trays should be used where possible. Cables should also be terminated in floor standing cabinets and labelled for easy identification.

Risks or hazards must be clearly marked.

5.3.3. Security

ICT rooms must be physically secure and access will be through an electronic system which provides a log of successful and failed attempts at entry together with a lock and key system. All failed attempts should be investigated and appropriate measures taken to address these. The entrance to the ICT rooms should also be fitted with a security burglar door.

All windows to the ICT rooms should be locked at all times.

5.3.4. Power

The supply of appropriately rated power outlets must be adequate to ensure safe and secure connections from the equipment to source. Overload protection must also be supplied.

When any changes are made to equipment within the ICT room the electrical loading must be checked to confirm that the supply remains adequate.

All equipment located in Category 1 ICT rooms must have UPS protection and, where it is practical to do so, generator backup. The UPS must be capable of supporting all the equipment inside the ICT room.

Power backup for equipment in Category 2 and 3 rooms must as a minimum consist of a local UPS with sufficient capacity to provide power backup for long enough to power down all equipment in the room.

5.3.5. Fire

All ICT rooms which have a fire risk must be protected by an early warning mechanism for fire consisting of smoke detectors or heat detectors integrated into the building fire alarm system. On activation the system must raise an audible alarm and cut the power supply to the room.

Category 1 rooms should have an automatic fire extinguishing system that can be activated out of hours and manually when staff is present. All other ICT rooms should as a minimum have CO2 hand held extinguishers available at the entry point to the room where practical.

All ICT rooms must comply with all relevant health and safety legislation and have good access to appropriately signed fire exits.



5.3.6. Air Conditioning

Category 1 rooms must have an air conditioning system that operates 24 hours a day 7 days a week. It should be designed to keep the room to within the IT manufacturers' recommended specifications for temperature and humidity throughout the year.

Category 2 rooms should have air conditioning appropriate to:

- the practicality of having a system installed
- the severity of temperature and humidity extremes
- what equipment is located in the room

5.3.7. Environmental control and monitoring

It is desirable to monitor temperature, humidity, power and cleanliness in category 1 and category 2 rooms, so that potential problems with air conditioning equipment and power supplies can be anticipated.

5.3.8. Lighting

Adequate lighting must be provided.

5.3.9. Cleaning

A periodic program of specialist cleaning should be in place for all ICT rooms. The frequency of cleaning must be appropriate to the environment and include under floor and above ceiling cleaning where there is a raised floor and false ceiling.

Staff using the rooms must keep them rooms clean and free of unnecessary contamination.

5.4. Security access to ICT rooms

The ICT personnel should know all locations containing ICT equipments. For this purpose a list of ICT rooms and authorized staff should be kept, including staff and contractors granted temporary permits.

The ICT Manager should grant authorization for accessing the ICT rooms for the following purposes:

- Operation, housekeeping, testing or storing of equipment within the room

- Maintenance of or upgrades to ICT equipment or environmental facilities within the room
- Management or audit

A register of all ICT rooms' keys issued and the holder thereof should be kept. The holders of the keys should sign the key register at the time that the keys are issued to them. In the event of loss or theft of any key immediate steps should be taken to prevent such key from being used again.

5.4.1. Rules for Executive Managers, Managers, and Staff members

The following rules should be followed on accessing the ICT rooms:

- The ICT division must ensure that the list of people authorized to enter them is kept up to date.
- All holders of ICT room's keys are totally responsible for those keys and should not loan them to anyone else.
- A person entering a secure room will not permit anyone not authorized to do so to enter the room.
- ICT rooms must never be left unattended unless they are fully secured to prevent unauthorized entry.
- The Manager of temporary staff requiring access to secure areas is responsible for ensuring that the person is aware of and complies with this procedure.
- Any person suspecting any form of security breach must report the event to the ICT Manager. This includes but is not limited to unauthorized entry, doors left open, locks not working, doors left unlocked or not closing properly, fire exit break glass broken, security codes divulged to unauthorized personnel, lost security ICT room keys.
- Anyone noticing suspect or unknown personnel in an ICT room must immediately either challenge the individual directly, or report the incident to the ICT Manager.

Any instances leading to security breaches resulting from staff not following the above guidelines may be considered a disciplinary issue.



5.5. Security of Removable Media

5.5.1. Backup Media

5.5.1.1. Storage

All data backup tapes must be stored in a secure location and this environment must be conducive to storage of magnetic media and operational use of computer equipment. If this is not possible then backup media must be allowed time to re-acclimatise to operational conditions before use. As a guide, providing the media has not been subjected to severe extremes of temperature, 4-6 hours should suffice.

5.5.1.2. Lifetime

Media in use for performing backups and archives should not exceed the manufacturer's recommendations on the useful lifetime.

5.5.1.3. Off-site storage

All backup media taken off-site should be logged in and out to ensure that all copies of data can be located if required, and off-site depositories can be audited.

5.5.2. Media in transit

Computer media can be vulnerable to unauthorised access, misuse or corruption during transportation. The following controls should be applied to media in transit between sites:

- reliable transport or couriers should be used with adequate insurance cover;
- packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications;
- media should be held in secure containers and tamper proof packaging that reveals any attempt to gain access.

5.5.3. Archives

Archives will be performed as ad hoc backups and will have a specified retention period, an owner and be securely stored with proper identification linked back to a media reference library or similar as described below.

5.5.4. Identification of media

All formal backup and archive media must be clearly labelled. The label will contain a clear link to reference information recorded about the media in a reference library, database or manual set of backup / archive log records. The type of information recorded will be:

- a cross reference number back to the media;
- cycle revision number - if in a rotation cycle;
- date the backup was performed - unless this can be referenced back to the rotation cycle in the logs;
- if an archive owner and retention date.

The identification system employed must avoid the use of descriptive labels. The data stored on the media must not be identifiable from its label.

The systems used to record the reference information about backup and archive media must be stored securely and if necessary with any off-site copies of the media so that reference can be made back to media in the event of disaster.

5.5.5. Recovery of data

As a matter of course operational staff must regularly test the backup/archive tapes to ensure that the tapes can be read and can be relied upon for emergency use when necessary. If normal procedures do not use backup tapes for restores on a fairly regular basis then routine random tests should be performed at least weekly.

5.5.6. Electronic media disposal

Municipal and end user floppy disks, CDs and all forms of tape media must be destroyed by a process that ensures that data cannot be recovered at the end of the destruction process. An ICT equipment and media disposal register should be kept where all ICT equipment and media disposals are recorded. The register should indicate what steps were taken to ensure that the guidelines as contained in this policy have been complied with including the removal of all licensed software and the authorisation for such disposal.

Hard disks in servers and PCs that are to be removed by a third party for replacement or maintenance should be either removed or destroyed or low-level formatted prior to re-use internally or by third parties who are subject to strict confidentiality clauses in their contracts.



6. System access control

6.1. Objective

To ensure that access to computer services and data is based on business requirements, and that access granted is consistent with job descriptions and requirements.

6.2. Policy statement

This area covers a wide area of activities

- Business requirements for access control should be defined and documented. System owners should provide the ICT division with a clear statement of the business requirements for system access, so that the ICT division can control access to ICT services and data.
- Procedures addressing user access should cover all stages in the life-cycle from initial registration of new users to their de-registration once access is no longer required. Users should have access only to those functions and information that they require to perform their duties
- Management should periodically conduct a formal review of users' access rights. Special attention should be given to privileged access rights that allow users to override system controls.
- Employees should follow good practices to protect password integrity in the initial selection and ongoing use of passwords.
- Network services, remote and external connections to the network should be centrally controlled and the access privileges provided should be limited to those services required for business purposes.
- All network logons should require a unique user ID and password to ensure that only authorized users gain access to the network.
- The use of powerful system tools should be limited to those who need them and such use should be closely monitored.

6.2.1. Security requirements for ICT projects

An analysis of security requirements must be carried out at the requirements analysis stage of each business application development project. Statements of business requirements for new business applications, or enhancements to existing business applications must specify the requirements for security controls. Such specifications normally focus on the automated controls to be incorporated in the system, but the need for supporting manual controls must also be considered.

These considerations must also be applied when evaluating software for business applications.

Security controls must reflect the business value of the information assets involved, and the potential business damage that might result from the failure or absence of security.

6.2.2. User & access rights

A formal user registration and deregistration process should be in place and must operate effectively. It should include appropriate authorization procedures, a periodic check for redundant ID's and procedures for their removal. Only employees that are on the payroll of the municipality are authorized to apply and be granted with the network access rights. The procedure should ensure that user access rights to the municipality's systems, data and business applications are:

- In line with the user needs (need to know principle)
- Clearly defined in a formal access request
- Authorized by the user's Executive Manager or Divisional Manager or his delegated official
- Timely changed when a user's responsibilities are changed
- Timely removed when a user leaves the municipality

6.2.3. Password, user ID and access rights administration

Formal standards for password management, user ID's and user access rights should be in place and implemented.

Controls should be in place to provide:

- Reasonable assurance that the use of system utilities is limited to authorized individuals and monitored
- Reasonable assurance that access to program source code is limited to properly authorized individuals
- Reasonable assurance that sensitive systems identified are isolated appropriately.
- Adequate guidance for end user responsibility for password management should be in place and operating effectively.



Passwords should comply with the following

- Passwords should be at least 7 characters long
- Password changing should be enforced with a minimum frequency of every 30 days
- Intruder detection should be enabled to out further login attempts after 3 failed attempts. The timeout period before the login counter is reset should be 1 hour, and the account should be locked for at least 12 hours in the event of 7 failed attempts.
- Where possible within the Network Operating System the following should also be enforced
 - Password re-use should be prevented for an agreed number of changes
 - A mixture of alphanumeric and numeric characters or a complete pass phrase should be required
 - There should be a list of banned 'trivial' passwords, enforced automatically

The password management process should include:

- Secure delivery of initial and temporary password
- Immediate forced password change
- Positive identification procedures in emergency situations
- Positive acknowledgement of password receipt

6.2.4. Security monitoring

Security monitoring should be performed on a regular basis following a formal procedure for regular security monitoring. Security monitoring should include:

- Periodic checks on redundant use ID's
- Periodic checked on user access privileges
- Periodic checks on security access logs



- Periodic checks on the use of powerful user ID's

A handwritten signature in black ink, consisting of several stylized, overlapping loops and lines, located in the bottom right corner of the page.

7. System development and maintenance

7.1. Objective

To ensure that security is built into ICT systems

7.2. Policy statement

It is the municipality's policy that an adequate change control process should be implemented to provide reasonable assurance that any changes made to the municipality's systems and applications in the operational environment are always identified, properly authorized, tested, approved, implemented and documented.

At the minimum, the change control process should include the following components:

- Initiation and approval of a change or development project
- Product development
- End user acceptance testing
- Release planning

7.3. Initiation and approval of a change or development project

Any software changes or new developments must be formally initiated through formal change requests. All change requests issued should be checked for validity, duplicates and formally approved by the appropriate personnel. Only formally approved change request forms should be considered as triggers for initiating development projects.

7.4. Product development

Product development should include the following components:

- Requirements analysis
- Developments approach (methodology, standards)
- Module testing
- System testing



7.5. Requirements analysis

Security countermeasures are substantially cheaper and more effective if incorporated in application systems at the requirements specifications and design stages. All security requirements, including the need for fallback processing, should be identified at the requirements phase of a project, justified, agreed and documented as part of the overall business case for an information system.

7.6. Development approach

Changes made to software must be performed in a separate environment from the production environment. A development methodology, containing standards and guidelines for system development by ICT officials should be available and strictly followed. Control should be in place to assure that support programmers give access only to those parts of the system that are necessary for their work.

7.7. Module testing

Every individual programmer is responsible for the performance of module tests on the programs developed. Module tests need to be performed in an environment separate from the production environment. They do not, however, need to be formally approved by appropriate personnel

7.8. System testing

System testing should be performed in a separate environment from the production environment. Formal system test plans and scripts should be drawn up based upon the results of the requirements analysis. System testing usually requires test data to be as close as possible to the live data. Test data should be protected and controlled. The use of live personal data should be avoided. If such data is used it should be depersonalized before. System test results should be formally reported and approved by the appropriate personnel.

7.9. Acceptance testing

Acceptance testing should be performed by end users in a separate environment from the production environment. Formal acceptance test plans and scripts should be drawn up based upon the results of the requirements analysis. Acceptance testing usually requires test data to be as close as possible to the live data. Test data should be protected and controlled. The use of live personal data should be avoided. If such data is used it should be depersonalized before use. Acceptance test results should be formally reported and approved by the appropriate personnel.

7.10. Release planning

Formal procedures for the implementation of new product releases should be available and must ensure that only tested and formally approved programs are taken into production environment. Special attention should be given to:



- End user sign-off including sign off for specific security requirements
- Technical change management; program transfer from test to production environment only to be executed by authorized officials.

A handwritten signature in black ink, consisting of a stylized, cursive script that is difficult to decipher. It appears to be a personal or official signature.

8. End user computing policy

8.1. Objectives

This document states the policy with respect to the use of computer resources by the municipality's users

8.2. Policy statement

Computer system resources and associated data are business critical municipal assets. Sufficient measures should be taken to ensure that all the end users use these assets appropriately without unduly exposing the municipality to security threats. All end users should be made aware of the supporting security standards and procedures related to End User Computing and violation of the security standards may lead to the disciplinary action up to and including termination of employment


8.3. Internet use

Users of the municipality's Information Technology resources should take note that these assets are intended for business use and the exploration of the internet should not have a detrimental effect on the business activities of the municipality. Incidental, occasional personal use is permissible so long as:

- It does not consume more than a trivial amount of system resources
- It does not interfere with the productivity of the individual.

8.3.1. Internet usage standards

- Users are expected to respect the privacy of others
- To respect the legal protection provided by copyright and license to programs and data
- To respect the integrity of computing systems, users may not harass other users or infiltrate a computer system and/or damage or alter the software of a computer system
- The municipality may at any time determine as to whether particular uses are or are not consistent with the municipality's business needs and may block traffic to particular internet sites



- Malicious use of any computer or computer system is not allowed, use should be consistent with guiding ethical statements and accepted community standards
- The internet may not be used to violate applicable laws or regulations
- The use of the internet or any other network in a manner that precludes or significantly hampers its use by others is not allowed.
- Use of the network or internet for any unauthorized recreational activity namely games, pornography, and any other related activities are not permitted.
- Users are not allowed to transmit any material either as the message or as attachments to a message, which in the municipality's sole discretion, are unlawful, obscene, malicious, threatening, abusive, libelous, and hateful or encourage conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of a municipal policy. Among those that are considered offensive are any messages that contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

8.3.2. Anti-virus measures

Anti-virus programs should be active at all times when a computer is utilizing any municipality network resources. Internet file downloads from unverified sources should be scanned for viruses before being opened as should suspect data from any other source.

8.3.3. Monitoring of Internet use

The municipality reserves the right to examine, at any time, without prior notice, e-mail, personal files and any other information that may be stored on municipal computers or network. The municipality can also monitor Internet usage through reviewing sites visited by users and examining files that are downloaded.

8.3.4. Internet security awareness

As the Internet is an insecure public domain no municipal information may be sent through the Internet unless it is specifically classified as public domain information.

Unless prior approval has been obtained no employee may set up connections that allow non-municipal employees access to the municipal systems information.

8.3.5. Additional Connections to the Internet

The municipality offers additional network tools like 3G cards to selected employees to help enable remote internet connection and access to emails from remote locations. The usage of these 3G cards is governed by this Internet User



Policy and such 3G cards users must make sure that they utilize them for official purposes.

3G cards are more vulnerable to virus attacks and all other security risks, as they are not protected by Lepelle-Nkumpi Municipality network security systems. To exercise control over security risks, all users connected to the LNM network are prohibited to connect their 3G cards whilst on the network. 3G cards are only allowed to be used at the remote locations or away from the office network.

3G cards are meant for internet access only and shall not be used for any other purpose like making phone calls. If a 3G card user is found using it for making phone calls, he or she will be liable for any costs incurred and might be subject to disciplinary actions.

8.3.6. Who qualifies for 3G cards

Municipal Manager

Executive Managers

ICT Manager

Network Controller

Employees who are authorized by Departmental Managers due to the nature of their work, like if they work with the municipal Financial System.

8.3.7. Internet Security Policy Statements

No configuration or enabling of other connections to the internet via modems, wireless networks and cell phones is allowed on municipal computers.

Access to the municipal network is limited to only the organs of state, and any other government entities and no remote or external connectivity is allowed.

No Remote (dial-in) Access is permissible due to security risks associated with dial-in and out facility.

- Only those employees who have received department management approval may access the Internet via the municipality's facilities. Automatic access to the Internet is not a right, and access can be revoked if it is found that misuse of the facility is occurring.
- Whenever an employee posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position of the municipality.

- Unless expressly authorized by the Municipal Manager, when using Municipality information and/or systems, all employees are forbidden from participating in Internet discussion groups, chat rooms, or other public electronic forums except for work related purpose.
- Users shall not advertise, promote, present, or otherwise make statements about municipality products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Municipal Manager.
- Although the Internet is an informal communication environment, the laws for copyrights, patents and trademarks apply. Employees using Municipality internet or communication systems shall:
 - Resend material only after obtaining permission from the source.
 - Quote material from other sources only if these other sources are identified.
 - Reveal internal municipality's information on the Internet only if the information has been officially approved for public release by the municipality's Communication section.
 - When using the municipality's information systems, or when conducting municipality's business, employees shall not deliberately conceal or misrepresent their identity.
 - Information Communication Technology Division may prevent users from connecting with certain non-business web sites. The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.
 - No user or independent contractor to the municipality may use the available Internet, Intranet or E-mail services provided by municipality to access newsgroups, Internet web sites and FTP sites for unauthorized and/or unacceptable purposes such as, but not limited to:
 - The viewing and/or downloading of pornographic or obscene material of any nature;
 - All software and files down-loaded from internet sources via the Internet (or any other public network) shall be screened with approved virus detection software before being run or examined via another program such as a word processing package.
 - All users wishing to establish a connection with the municipality's computers via the Internet shall authenticate themselves at a firewall before gaining access to the municipality's internal network. Contact the Information Communication Technology Division for further information.



- Non-municipality's computers are prohibited from connection to the municipality's networks without specific written permission from the Municipal Manager.
- Dial out or connections to any non-municipality systems or networks while simultaneously connected to the internal network are prohibited.
- Do not run security-testing tools/programs against any Internet system or server.
- Dial up connections e.g. whilst traveling or from home based systems and laptop computers which are also utilized for municipal business must only be made via authorized dial up procedures which employ the use of firewalls and configured by Information Communication Technology Division.

8.3.8. Non-compliance

The municipality reserves the right to audit compliance with this policy from time to time. Disciplinary action for non-compliance may include dismissal. The municipality also reserves the right to suspend or permanently remove a user's access to some or all of the electronic services specified in this policy.

8.4. Use of Electronic Mail Facilities

This policy is established with regard to access and disclosure of internal and external electronic communication messages (e-mail) created, sent received or stored, vial the Internet or the municipality's intranet, by its employees, Managers, Heads of Departments and contractors using the municipality's e-mail systems.

It is the responsibility of each Manager, Unit Head and employees to ensure that use of the municipality's e-mail system complies with the guidelines as set out in this policy.

The e-mail system is the municipality's property and all copies of messages created, sent, received or stored on the system are and remain the property of the municipality. The municipality maintains its e-mail system solely for business purposes and may not be used to engage in improper or illegal activity. Incidental, occasional personal use is permissible so long as:

- It does not consume more than a trivial amount of system resources
- It does not interfere with the productivity of the individual (both sender and receiver)



Common courtesy and respect for the reader's dignity should always be observed in e-mail content. This is particularly necessary when expressing displeasure, dissatisfaction, or similar sentiments. Abusive or obscene language is forbidden.

8.4.1. General Requirements

The following actions and uses of the e-mail system are **expressly forbidden**:

- Sending of unsolicited bulk mail messages of a personal nature;
- Propagation of chain letters;
- Advertising of personal items;
- Use of private e-mail accounts for business related e-mails.
- Frivolous usage of the e-mail system, for reasons of either a business or private nature. This would include replies to task requests in the affirmative, such as, Mail sent "Please will you print and fax the attached document to Mr. A". A reply is then sent "Okay".
- Subscription to mailing lists, discussion groups, a list-server, or other such bulk mailing services, for private purposes;
- Subscription to third party mail systems and use of such mail systems from company premises, unless directly related to a business need or objective;
- Transmitting any material either as the message or as attachments to a message, that in the municipality's sole discretion, is unlawful, obscene, malicious, threatening, abusive, libelous, or hateful, or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of company policies. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
- Employees are not authorized to retrieve or read any e-mail messages that are not addressed to them. Employees shall not use any password or code, access a file, or retrieve any stored information, unless authorized to do so by an appropriate supervisor.



8.4.2. E-Mail Disclaimer

Users may not transmit personal opinions as those of the municipality, nor make any statement that may be construed to be a municipality statement. The following disclaimer should be included as a suffix to all e-mail messages to addresses external to the municipality:

E-Mail Disclaimer.

The information contained in this communication is confidential and may be legally privileged. It is intended solely for the use of the individual or entity to whom it is addressed and others authorised to receive it. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking action in reliance of the contents of this information is strictly prohibited and may be unlawful. Lepelle-Nkumpi Municipality is neither liable for the proper, complete transmission of the information did not contain in this communication nor any delay in its receipt.

8.4.3. Attachments to e-mail Messages.

Attachments to e-mail messages should be used sensibly. Transmission of large volumes of data in a message can have a drastic effect on the general level of service provided to all other users. If it is necessary to include attachments then these should be restricted to less than 10Mbytes in size when using internal mail, and 6 Mbytes in size when using any Internet addresses. Files larger than recommended above should be broken into separate "chunks" (usually zipped) and then transmitted as separate e-mail messages.

8.4.4. Size of the user's mailbox

The size of every user's mailbox is limited to 50Mb on the exchange server. When the user's mailbox reaches:

- 40Mb, a message will be displayed requesting the user to be clear the mailbox;
- 45Mb, the user will not be able to send messages, but will be able to receive them;
- 50Mb, the user's account will be disabled.

8.4.5. Non-compliance

The Municipality reserves the right to audit compliance with this policy from time to time. Any disciplinary action, arising from breach of this policy, will be taken according to the municipality's defined disciplinary code and procedures. Disciplinary action may lead to dismissal.



The municipality reserves the right to suspend or permanently remove a user's access to some or all of the electronic communication services specified in this policy. Any user whose mailbox is suspended will need to consult with their Executive Manager or Manager. Depending on the severity of the infringement, the Municipal Manager would also need to be consulted before re-instatement of the e-mail account. The Executive Manager will then issue a written authorisation to the exchange administrator to re-instate the account.

The municipality also maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages created, received, sent or stored on the e-mail system for any purpose. By using the municipality's e-mail system an employee recognizes the foregoing rights of the municipality and consents to them.

8.5. Anti-Virus Security

This document states the policy for the protection of the municipality's data from accidental or unauthorised modification, loss, or loss of confidentiality by viruses, Trojan Horses and other malicious code.

8.5.1. Policy Statement

Municipal data is a business critical municipal asset and requires a high level of protection at all times. Measures will be implemented to protect this asset against accidental or unauthorised modification by malicious code. Steps will be taken by the ICT division to provide as much security against viruses and other malicious code as is possible. However, reasonable precautions should be taken by every member of staff not to introduce unsupported or unverified software that may contain malicious code. Until data is copied to network servers, which is the responsibility of the ICT division, the individual user is responsible for the care of the data on their machine.

All incoming software should be regarded as possibly infected no matter what the source, including shrink-wrapped disks, CDs, files downloaded from other networks and attachments in mail. On discovery of malicious code members of staff must report it to the ICT division immediately and prevent the machine concerned from being used (including connection to the network) until it has been certified clean.

8.5.2. Requirements

The ICT division is responsible for determining the anti-virus software to be loaded on all the municipality's computers. End users are under no circumstances to:

- Disable the software;
- Load a different anti-virus package (unless authorised by the ICT division) or;



- Re-configure any settings on the software.

The ICT division is responsible for providing means for protecting information within their assigned area of management control. They are not responsible for the data on individual workstations or mobile PCs. This remains the responsibility of the user of that machine. End users should ensure that their virus definitions on their anti-virus software are updated at least once every two weeks.

8.5.3. Enforcement

Any violation of standards, procedures or guidelines established in support of this policy shall be brought to the attention of management for appropriate action. Such violation will be regarded as misconduct and may result in disciplinary action being taken against those responsible.

8.6. Use of computer hardware and software

End users must be made aware of and acknowledge their responsibilities for the safe keeping of ICT assets in their possession. This should be made before any use is made of such assets or possession taken thereof. A written declaration in this regard should be signed

8.6.1. Acquisition and allocation of computer equipment

At the request of the employee's manager, accompanied by a signed appropriate Application for ICT Equipment Form, computer equipment may be procured and an employee may have access to computer-based services. These are provided to assist the employee to fulfill his/her official duties and/or business activities. The ICT Manager sets the qualifying criteria.

ICT Division should be consulted or engaged in the procurement of all municipal ICT Equipments and systems for assistance in identification of systems, whether software or hardware, that are compatible to the ICT Infrastructure and also that are compliant to the adopted Master Systems Plan (MSP).

New equipment will be procured only if current equipment does not comply with the minimum standards set for the computer equipment. Printers are allocated in the same way but employees will be expected to share printers with other personnel.

In cases where an employee requires the allocation of non-standard equipment or software to fulfill their duties effectively, the employee's senior manager or head of the section must make a recommendation in the



form of a motivated submission to the ICT Division. The submission must include the details and cost of the software or equipment required.

9. MANAGEMENT OF IT EQUIPMENT

The ICT Division is responsible for the management of IT Assets and the asset Life Cycle management processes including standards, acquisition management and long range planning. Authority to acquire ICT assets is held by the ICT Division.

Disposal of all ICT Equipments should be done in consultation with the ICT Division with the purpose of testing and declaring the equipment outmoded.

9.1. STANDARDS

9.1.1. The ICT Division will specify the standard issue personal computer

To make for cost-effective use of equipment and software, the Municipality will standardize on a core set of software and hardware product requirements. The specifications will be set and revised from time to time by the ICT personnel. The standards will cover the following:

- Minimum specifications for current desktop computers. Users may only request new computers if their current computers do not comply with the minimum specifications set by the ICT Division.
- Hardware specifications for standard issue desktop computers, notebook computers and printers. Users will be issued with a computer that meets the standard. When the standard is raised, computers below the standard can be upgraded or replaced, if the computer is found to be inadequate by the ICT Division, it will be upgraded or replaced.
- The ICT Division will normally follow the standard set by the State Tender Board or SITA's Information Technology Acquisition center.

9.1.2. Non-standard items will not be supported



The ICT Division supports a large number of products - both hardware and software. To keep costs down IT Support limits the product range it is willing to support and provide training for. If an employee uses software that falls outside this product range, the ICT Division cannot guarantee support for such a product.

9.1.3. Allocation of personal computers as well as a laptop computer to employees

Employees are not entitled to both a laptop computer as well as a desktop personal computer (unless authorized by their Head of Department and the ICT Manager). An employee may not request that a laptop computer be procured, if such an employee is already in possession of a desktop personal computer and vice versa. If a person is in the possession of a personal computer and requires a laptop, the equipment will be cascaded to next line personnel. A written motivated submission stating reasons why the employee requires an additional laptop or personal computer shall be attached to the Standard Application form.

9.2. USAGE OF IT EQUIPMENT

9.2.1. Classification of Computer Users

Employees are classified into two categories according to the nature of their work. Standard users are employees who only use standard applications installed on their personal computers. High-level users are employees who use standard software and additional applications used in their divisions such as the Financial Systems.

9.2.2. Use of computer equipment for official purposes

Computer equipment is issued to employees for official duties and for Municipality's business or activities sponsored or authorized by the Municipality.

9.2.3. Use of computer equipment for non-official purposes



Occasional and brief use of computer equipment by employees for personal use is allowed, but not encouraged, subject to the following restrictions:

- Personal use should not hinder productivity.
- Only incidental amounts of employee time, time periods comparable to reasonable breaks during the day, should be used to attend to personal matters.
- Personal use should not cause the Municipality to incur a direct cost in addition to the general overhead.
- Employees may not install or use software that does not support official business or activities sponsored by the Municipality, such as games, screensavers, screen utilities, movies, songs not on original CD and pictures.
- Personal use shall comply with all other terms of this policy.

9.2.4. Storing of material on computer equipment

Users should take care not to expose the Municipality and its employees to materials or information that could be considered offensive. This includes words, images of any kind and recorded sounds (audio). If someone else accidentally sees material stored by an employee, the employee could face a charge of harassment. Regular harassment can create a hostile working environment for co-workers.

Storing of the following material is expressly prohibited:

- Discriminatory, intolerant or derogatory matter based on race, religion, gender, age, ethnic or social origin, sexual orientation, disability, physical condition, HIV status, conscience, belief, political opinion, culture, language or birth.
- Any form of violence, pornography, explicit nudity, sexual acts, gross depictions, religious content deemed inappropriate by other religious groups, militant or extremist material.

10. Laptop /Notebook Allocation



The use of personal computers and laptops has become an integral part of fulfilling an employee's daily task and responsibilities. To this end, the municipality provides employees with the access to personal computers or workstations to enable them to fulfill such duties and responsibilities.

In certain instances, the nature of an employee's job necessitates access to a notebook (portable personal computer) or handheld computer. This document serves to clarify the municipality's approach regarding Lepelle-Nkumpi provided notebooks. Management reserves the right to amend or provide exceptions to this document in specific instances.

The municipality will provide the following employees with Notebooks: -

Category 1

Mayor

Speaker

Chief Whip

Municipal Manager

Executive Managers

Managers;

Employees who are disabled and require special accommodation measures to enable them to full fill their normal responsibilities.

Category 2

Employees who require access to portable personal computers for the purpose of fulfilling their normal daily responsibilities

- In this case a motivation has to be submitted to the Information Communication Technology Division through the Executive Manager: Corporate Services.

Laptops remain the property of the municipality and must be returned on the employee leaving the employment of the municipality. The staff member is responsible for ensuring all appropriate steps are taken to avoid accidental damage or loss to the laptop. All other employees who are required to use or have access to



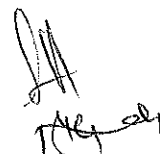
computers will only be given access to desktop personal computers or computer workstations.

10. PRINTERS

Printers will be allocated to officials depending on their specific needs. Color DeskJet printers will be allocated to those who frequently needs to print color documents, other officials will be required to use the central color printer.

11. MANAGERS'S RESPONSIBILITY

Managers have to monitor the use of computer equipments and software by officials within their departments. Managers must ensure that all their computer-using staff, temporary or permanent is made aware of this policy. The Managers are required to apply the policy to all those who report to them.

Handwritten signature and initials, possibly "SA" and "TAY" or similar, located at the bottom right of the page.

12. DON'T S AND DO'S

You are not allowed to

- Bring your home computer along to the office.
- Move your computer without informing the Information Communication Technology Division.
- Put your coffee/tea cup on top or closer to your computer.
- Disconnect your PC for a reason not known to the ICT unit.
- Install a third party software or non-standard software, unless authorized to do so.
- Install computer games or other entertainment software.
- Repair or perform any form of upgrade to the computer equipment.
- Swap computer equipment with other officials.
- Exchange or swap passwords

You must

- Switch off your computer when you knock off.
- Be logged into the network when using a computer.
- Obtain a permit before taking an equipment offsite, unless it is a notebook officially allocated to you.
- Always keep your desktop computer tidy.
- Inform ICT unit if you suspect there is something wrong with your equipment before it is too late.
- Report any unlicensed or suspected non-standardized software to the Information Communication Technology Division.



The terms of this policy shall take effect on the date of approval by the Lepelle-Nkumpi Municipality Council.

Document Name: **INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICY**

Reviewed By:  Date: 01-04-2014
ACTING MUNICIPAL MANAGER

Recommended by

Portfolio Committee: Corporate Services

CHAIRPERSON Date: _____

Approved by Council:  Date: 01-04-2014

(Speaker)

RESOLUTION NUMBER: 7.1.4.02/2014

ICT SECURITY POLICY 2014/2015