

Dr NDZ Municipality



ICT Security Control Policy

	Version
	1

ICT Manager

Dr Nkosazana-Dlamini Zuma Local

Municipality

Main Street

Creighton

Telephone(039) 833 1038

Facsimile(039) 833 1179

Website www.ndz.gov.za

Page 1

ICT Security Control

ICT Security Control Policy

ICT security is characterized as the preservation of the confidentiality, integrity and availability of information and associated assets. The ICT Security Control Policy is intended to provide a common basis for developing organizational security standards and effective security management.

Table of Contents

1. Version Control	4
2. Definitions.....	5
3. Introduction.....	6
4. Objective	6
5. Scope/Audience	7
6. Roles and Responsibilities	7
7. Appointment of IT Steering Committee.....	7
8. Administrative Controls	8
9. Physical controls.....	9
10. Access control	11
11. Data Security Control	15
12. Internet	15
13. Authority to speak on the behalf of DrNDZ Municipality	16
14. Integrity of Dr NDZ Municipality's Image.....	16
15. Security	16
16. Electronic Mail (Email)	17
17. Unacceptable Practices.....	17
18. Ownership and Classification of Data.....	18
19. Wireless Security	19
20. Official Website	20
21. Protocols	21
22. PC Support.....	22
23. Disaster Recovery Plan	22
24. IT Training and Security Awareness	22
25. Acceptance of and Compliance with the IT Security Controls Policy	23
26. Policy Violations.....	23
27. Policy Review	23
28. Publishing the policy	23
29. Appendices.....	23
30. Doctor Nkosazana Dlamini-Zuma Municipality Approval and Sign-Off	24

1. Version Control

Full Title	DR Nkosazana Dlamini-Zuma Municipality's IT Security Control
Short Title	IT Security Control Policy
Author(s)	
Version	01
Author(s)	
Version	02
Authorized By	Council
Authorization Date	
Effective date	

2. Definitions

Term	Meaning
IT	Information Technology
ICT	Information and Communication Technology
Municipality, the	Dr Nkosazana Dlamini-Zuma Municipality
KZN	Kwazulu-Natal
IM	Information Management
AP	Access Point
IPME	Institutional Performance Monitoring and Evaluation
DrNDZ	Dr Nkosazana Dlamini Zuma

3. Introduction

In order to promote a working environment that is conducive to teamwork and productivity, it is essential that all users understand their roles and responsibilities with regards to Information Technology (IT) security and adhere to the security requirements of DR Nkosazana Dlamini-Zuma Municipality. IT security is therefore characterized as the preservation of:

- **Confidentiality** - Ensuring that information is only accessible to those individuals who are duly authorized to have access to it.
- **Integrity** - Safeguarding the accuracy and completeness of information and processing methods.
- **Availability** - Ensuring that authorized users have access to information and associated assets as and when required.

4. Objective

The objectives of the IT Security Control Policy are to:

- 4.1. Clarify to all users their responsibilities regarding the security of Dr NDZ Municipality's information and computing resources.
- 4.2. Define the potential risks and dangers for the Municipality in the event of misappropriation and abuse of computing equipment by users.
- 4.3. Maintain an appropriate level of physical and logical security to safeguard IT systems and resources against unauthorized use, modification, disclosure or loss to preserve the integrity of the Municipality's IT environment.
- 4.4. Regulate the professional and effective use of computing equipment within the Municipality, as well as between the Municipality and its external entities.
- 4.5. Establish a standard for the creation of User ID's and strong passwords, the protection of those passwords and the frequency of change thereof.
- 4.6. Identify the persons responsible for maintaining the security requirements.
- 4.7. Establish management direction, basis of procedures and requirements to ensure the appropriate protection of the Municipality's information and equipment resources.
- 4.8. Ensure that the investment in information and equipment resources is properly managed.
- 4.9. Ensure that all systems are optimally utilized in its full capacity to the best advantage of Dr NDZ Municipality.

5. Scope/Audience

This policy applies to all employees, consultants, councilors and temporary staff who access Dr NDZ Municipality's computer networks with an organization-owned workstation and are responsible for an account (or any form of access that supports or requires a User ID and a password) on any system that resides at any of the Municipality's facilities, has access to the network, or stores any non-public organizational information. All employees need to be aware of security risks and vulnerabilities in order to create organization-wide security consciousness.

6. Roles and Responsibilities

The table below describes the key stakeholders and their respective roles and responsibilities in terms of IT Risk Management.

Table 1: Roles and Responsibilities

Role	Responsibilities
ICT Manager	The ICT Manager must ensure that effective IT Security Controls are established within the IT Unit
ICT Officer	The IT Officer must implement, where possible, all IT Security Controls established by the ICT Manager.

7. Appointment of ICT Steering Committee

DR NDZ Municipality shall appoint an ICT Steering Committee that is required to discuss and approve IT-related improvements or changes in the IT environment and infrastructure.

8. Administrative Controls

8.1. General Controls

- 8.1.1 The ICT Manager will, on recommendation of the IT Steering Committee, issue guidelines on the use and application of Dr NDZ Municipality's network and shall monitor compliance with these guidelines, which must be strictly adhered to by all users of any IT systems.
- 8.1.2 The required administrative controls applicable to systems will be included in these guidelines and will comprise the following:
 - 8.1.2.1 Physical controls over computer hardware, backups and software;
 - 8.1.2.2 Access controls;
 - 8.1.2.3 Data security controls; and
 - 8.1.2.3 Internet and email usage controls.

8.2 Programming and Documentation Standards

- 8.2.1 Only the ICT Manager, on recommendation of the IT Steering Committee, may liaise with IT software suppliers to provide developers for the development or modification of applications used by Dr NDZ Municipality.
- 8.2.2 The ICT Manager shall keep a register of all such requests for amendment and/or enhancement of Dr NDZ Municipality software and hardware, and shall inform the relevant users of any changes.

8.3 Insurance

- 8.3.1 The Finance department shall ensure that appropriate and adequate insurance cover is obtained in respect of all components of Dr NDZ Municipality's IT operations.

8.4 Reporting

- 8.4.1 The ICT Manager shall report quarterly to the ICT steering committee on the general use and application of the IT network, indicating in such report whether existing administrative controls need to be reviewed or amended, specifying operational problems of material importance which have arisen during the month to which the report relates, and indicating how such problems have been or are being addressed.

8.5 Audits

- 8.5.1 The ICT Manager, in consultation with the Chief Financial Officer (CFO), shall arrange audits of the IT systems on a periodic basis.
- 8.5.2 These audits may be conducted by either the internal or external auditors (or both), provided that sufficient budgetary provisions have been provided for.
- 8.5.3 The findings of such audits may be included in the audit report to the IT Steering Committee, or if findings are significant then they must be reported to the Audit Committee.

9. Physical controls

Physical controls with regards to Dr NDZ Municipality's IT network relate to measures which must be put into place to ensure the physical security and protection of all relevant computer hardware, software, manuals and the computer room. The physical controls are required to provide protection against natural hazards, as well as the risks of theft and/or negligence on the part of Dr NDZ Municipality's officials.

9.1 Hardware Controls

- 9.1.1 Where personal computers have been allocated to officials, such officials shall accept that these computers must be used to fulfil operational functions within the Municipality and that their use is restricted to such official functions only.
- 9.1.2 All computers fitted with locking cases must be kept locked at all times.
- 9.1.3 No hardware may be installed or removed by any municipal official without prior consent and authorization or direction from the ICT Manager.
- 9.1.4 No hardware may be removed by any official from municipal premises without the prior written authority of the ICT Manager in consultation with Chief Financial Officer (CFO). The ICT Manager shall keep such written authority on file, and the official who wishes to remove the relevant hardware must have a copy of such authority for inspection when required.
- 9.1.5 Any malfunctioning computers must be immediately reported to the ICT Manager by the official to whom such equipment has been allocated and the ICT Officer shall attend to the required repairs or replacement of the equipment, but subject to the necessary provision having been made in the budget.
- 9.1.6 Given the significant cost of laser and ink jet printing, officials to whom the use of printers has been allocated must ensure that all printing is kept at a minimum or

rather in fast draft print quality. Wherever possible, screen previews should be used rather than physical printing. Original toners and inkjet cartridges must be used when printing is necessary, as not only may the compatible or refilled products void Dr NDZ

Municipality's warranty in respect of the equipment, but they can also (in given circumstances) damage the printers.

9.2 Software Authorization and Licensing

9.2.1 The ICT Manager shall maintain a list of approved software's to be used on the IT network, as well as the number of licenses owned and the number of copies of such software loaded onto the system.

9.2.2 Only authorized and licensed software listed on the approved software listing may be loaded onto Dr NDZ Municipality's computers, and this may only be implemented with the consent and supervision of the ICT Manager.

9.2.3 The ICT Manager shall further ensure that this authorized list, referred to as the "Approved Software List", is reviewed and updated periodically in order to address any new software which is released into the market that may be relevant to Dr NDZ Municipality and as the need for new or additional software arises.

9.2.4 No software may be downloaded through the Internet or via email. Also, pirated software by any official will not be permitted whatsoever.

9.3 Standard Applications

9.3.1 A new user is entitled but not limited to the following standard applications upon receiving a new computer or if the user is new to the municipality:

9.3.1.1 Antivirus Software;

9.3.1.2 Acrobat Reader;

9.3.1.3 MS Office;

9.3.1.4 Internet;

9.3.1.5 Specialized Applications; and

9.3.2 A user is entitled to the municipality's applications once duly authorized.

9.4 Computer Manuals

- 9.4.1 The originals of software, hardware, systems manuals and guides shall be kept by the IT Manager with relevant licenses and discs.
- 9.4.2 The IT Manager shall further ensure that the manuals and release notes are updated with each new release installed on the systems.

9.5 Server Room

- 9.5.1 Only the ICT Manager and authorized personnel shall ordinarily have access to the server room.
- 9.5.2 The server cabinet and computer room shall be kept locked.
- 9.5.3 Access to the server room is via biometric (finger print) and keypad access.
- 9.5.4 The ICT Manager shall ensure that adequate fire prevention and extinguisher systems are installed in the server room, and that this equipment is regularly checked and maintained.
- 9.5.5 No official may tamper with such equipment, and no official may remove any such equipment from the computer room other than for the purpose of having it tested or_ serviced.
- 9.5.6 The IT Manager shall ensure that a properly designed, maintained and operated air conditioning system is installed in the server room.
- 9.5.7 The ICT Manager shall regularly test or have tested the Uninterrupted Power Supply (UPS) in order to ensure that it is maintained in an operational condition.

10. Access control

10.1 General

- 10.1.1 Access control is necessary to restrict unauthorized user access to any portion of the IT network or to any particular component of the system. It is therefore necessary that the bona fide user, in order to gain access, must first be authorized, i.e. the access of such user to the system must be properly authenticated.

10.1.2 Access to the IT network comprises three steps:

10.1.2.1 Physical access to a workstation;

10.1.2.2 Access to the system; and

10.1.2.3 Access to specific commands, transactions, programmers and data within the system.

10.2 Physical Access to Systems

10.2.1 After the user has switched on his or her computer, the user must enter a password to gain further access to systems.

10.3 Access to specific Commands, Transactions, Programs and Data within the System

10.3.1 The IT Manager shall set access level priorities in accordance with the job descriptions of the officials concerned and to comply with further specific requirements of the officials from the relevant business unit.

10.3.2 Access level and amendment priorities shall be set out in writing by the ICT Manager.

10.4 User Passwords

10.4.1 Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Dr NDZ Municipality's entire network.

10.4.2 All Dr NDZ Municipality's employees, consultants and temporary staff with access to the Municipality's systems are responsible for taking the appropriate steps (as outlined below) to select, maintain and secure their passwords at all times and never use an account assigned to another user, as they will be held responsible for total use or misuse of their account.

10.4.3 All officials, to whom user passwords have been allocated, must ensure that these passwords are properly safeguarded.

10.4.4 Under no circumstances may the employee share any user password with colleagues.

10.4.5 Passwords are used for various purposes at DR NDZ Municipality. Some of the more common uses include: user level accounts, web accounts, email accounts, screensaver protection, application logins and logins to IT Hardware.

10.4.6 All users should be aware of how to select strong passwords. Hence, the following password guidelines must be adhered to by all users on all servers and computers within Dr NDZ Municipality:

10.4.6.1 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

10.4.6.2 Passwords must not be inserted into email messages or other forms of electronic communication.

10.4.6.3 Passwords should not be a word in any language, slang, dialect or jargon.

10.4.6.4 Do not use the same password for the Municipality's accounts as for other non-organizational access (e.g. personal account, option trading, benefits, etc.).

10.4.6.5 Users must not use the "Remember Password" feature for applications (e.g. Internet Explorer, etc.), and must not write passwords down.

10.4.6.6 Users must not store passwords in a file on any computer system (including laptops or similar devices).

10.4.6.7 Users must avoid using the same password for multiple applications.

10.4.6.8 If an account or password is suspected to have been compromised, the user must report the incident to the ICT Manager and change all their passwords accordingly.

10.4.6.9 If a user is requested to provide their password details to the ICT Manager, they must ensure that they monitor the actions performed. Thereafter, the user should change their password immediately once the ICT Manager has left.

10.4.6.10 Where possible, systems have been configured to follow DR NDZ Municipality standards. The Municipality's requirements for password settings should be as follows:

10.4.6.10.1 A minimum of eight (8) characters in length;
10.4.6.10.2 Must be changed every 30 days;

- 10.4.6.10.3 A password history of (twenty-four) 24 generations should be maintained;
- 10.4.6.10.4 Password complexity must be enabled and consist of alphanumeric and special characters;
- 10.4.6.10.5 User accounts are set to lockout after 3 unsuccessful login attempts; and
- 10.4.6.10.6 Users should not use their usernames as passwords.

10.4.6.11 It is therefore of utmost importance that users follow the guidelines below on password construction and safeguarding their password in order to minimize the threat of others obtaining their passwords.

10.4.6.11.1 Personal details, such as spouse's name, license plate, ID number or birthday, must not be used.

10.4.6.11.2 Words in a dictionary, derivatives of user ID's and common character sequences such as "123456" must not be used as well.

10.4.6.11.3 Passwords should not be based upon month/ year combinations such as "jan09" or "april2009". Hackers use these types of words in attempts to guess passwords.

10.4.6.11.4 Users must not use cyclical passwords. For example, users should not add a numeric at the end of the password in sequence.

10.4.6.11.5 Passwords must not consist of all identical numeric or alphabetic characters, such as: "11111111" or "aaaaaaa".

10.4.6.11.6 Employees must never share their passwords with anyone, including the IT Manager, administrative assistants or secretaries.

10.4.6.11.7 All passwords are to be treated as sensitive Municipal information.

10.4.7 Additional configuration settings for Active Directory Server

10.4.7.1 A minimum password age of 30 day;

10.4.7.2 Accounts should be set to lockout indefinitely (until the ICT Manager unlocks);

10.4.7.3 Accounts are set to lockout after 3 invalid log-on attempts.

10.4.8 Users must take note that for all activity performed using their user name and password, they will be held accountable and may face disciplinary action in the event of misuse.

10.4.9 Users must take note of and adhere to the following "Don'ts":

10.4.9.1 Do not reveal a password over the phone to anyone.

10.4.9.2 Do not reveal a password in an email message.

10.4.9.3 Do not talk about a password in front of others.

10.4.9.4 Do not hint at the format of a password (e.g. "my family name").

10.4.9.5 Do not reveal a password on questionnaires or security forms.

- 10.4.9.6 Do not share a password with family members or colleagues.
10.4.9.7 Do not reveal a password to co-workers while on vacation.

Annexure A

Password Reset Form



A Better Place for All

ICT User Password Reset Form

Purpose

This form is to be filled in for any change in user permissions. Relevant fields are to be filled in, and the form is to be signed off by the relevant user, the ICT officer implementing the change and may be reviewed by the ICT Steering Committee or a relevant HOD.

☐

New User

☐

User Removed

☐

User Change/Password Reset

User Name: _____

Relevant System (Email, SAMRAS, File Server): _____

Change Required: _____

Change Approved By: _____

Date: _____

Change Done By: _____

Date: _____

User Signature: _____

ICT/Procurement: _____

Officer Signature:

Reviewer Name

Reviewer Signature

Review Date

11. Data Security Control

11.1 Privileges and Exposure

11.1.1 Access by users to Dr NDZ Municipality's IT systems shall be restricted in accordance with the job descriptions of officials concerned.

11.1.2 Users are responsible for the protection of sensitive information by ensuring that only officials whose duties require such information are allowed to obtain knowledge of such information while it is being processed, stored or in transit.

11.2 Backups

11.2.1 Backup procedures will be determined by the ICT Manager and communicated to all relevant users accordingly.

11.2.2 Backup procedures shall be adhered to by all users on the system.

11.2.3 To protect Dr NDZ Municipality's information resources from loss or damage, users are responsible for backing-up information stored on their machines.

11.2.4 Backups will be stored in a secure site.

12. Internet

12.1 Use of Internet

12.1.1 Internet access and related IT resources are provided to DR NDZ Municipality at significant cost and are made available primarily for business use.

12.1.2 Users who have access to the Internet shall use this access solely in connection with official responsibilities, including communicating with clients, working with related partners, local and provincial government agencies, providers of goods and services to Dr NDZ Municipality, and to also research relevant topics and obtain business related information which is of use to Dr NDZ Municipality.

- 12.1.3 Limited personal use on approved sites may be authorized when such access will be to the best advantage of Dr NDZ Municipality only.
- 12.1.4 All users who have access to the Internet shall conduct themselves honestly and appropriately, and respect copyrights, software licensing rules, property rights, privacy, and the prerogatives of others.
- 12.1.5 Officials who use the Internet shall ensure that intellectual property of others is protected and that Dr NDZ Municipality's resources are not misused, that information

and data security (including confidentiality where applicable) are at times respected, and that the Internet is not used for any form of abuse.

- 12.1.6 Every official using the Internet facilities of Dr NDZ Municipality shall identify himself or herself honestly, accurately and completely.
- 12.1.7 Officials using the Internet shall do so only when this is required to fulfil their official responsibilities and/or when they are authorized to do so.
- 12.1.8 Whenever an official downloads any file from the Internet, such a file must be scanned for viruses before it is run or accessed. If the official is uncertain as to the procedure to be followed, such official shall immediately seek assistance of the ITManager.
- 12.1.9 Live streaming of video and / or audio signals over the Internet is prohibited.

12.2 Internet Browser

- 12.2.1 Dr NDZ Municipality reserves the right to block and track all visited sites.

13. Authority to speak on the behalf of Dr NDZ Municipality

- 13.1. Only those officials who are duly authorized by the Municipal Manager to speak to the media, to analysts, in public gatherings or send external emails on behalf of DR NDZ Municipality may do so.

14. Integrity of Dr NDZ Municipality's Image

- 14.1. Officials who are authorized to speak on behalf of Dr NDZ Municipality, as set out in section 13.1 above, shall ensure that they honor the image and integrity of Dr NDZ Municipality at all times and do not engage in any unauthorized political advocacy.
- 14.2. Officials must ensure that, where inputs are provided on behalf of Dr NDZ Municipality to any news group or chat room, such inputs have been grammar and spell-checked, and that the inputs reflect the view of Dr NDZ Municipality (where applicable) rather than the personal opinions of the writer.

15. Security

- 15.1. Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, Internet address screening program or any other security systems installed by the ICT Manager or any IT suppliers to assure the safety and security of Dr NDZ Municipality IT network.
- 15.2. Any officials who obtain a password, which allows access to the Internet and/or the Municipality's IT network, shall keep such a password confidential, except if any occasion arises where any authorized technical support official requires knowledge of such password in order to solve a computer related problem.

- 15.3. As set out in 7.4 above, the present policy strictly prohibits the sharing of passwords between officials.
- 15.4. Logging onto the IT network or Internet with one's personal password, and then allowing another user to use or work on the Internet or the IT network, shall be viewed as an attempt to bypass official security procedure, and is strictly prohibited and will be dealt with accordingly.
- 15.5. Every authorized user shall sign all IT Security Policy Compliance Agreements provided to them by the ICT Manager before attempting to gain access to the Internet and/or the network.
- 15.6. The ICT Manager will review all Internet activities and analyze the relevant usage patterns. Thereafter, appropriate action will be taken on the user wherever any abuse of the system is evident.

16. Electronic Mail (Email)

- 16.1. Only authorized officials shall use the available email facility.
- 16.2. The ICT Manager shall scan all emails for any inappropriate content or offending words or phrases.
- 16.3. All copies of emails shall be kept as records.
- 16.4. Only authorized officials shall be permitted to receive attachments through the email system.
- 16.5. The ICT Manager shall maintain a list of prohibited and blocked email, and shall update and amend such list as circumstances require.
- 16.6. Dr NDZ Municipality reserves the right to monitor, access, retrieve, read, and/or disclose employee communications sent via the email system.

17. Unacceptable Practices

- 17.1. No official may display any kind of sexually explicit material on any municipal system. Furthermore, no sexually explicit material may be archived, stored, distributed, edited or recorded using any of Dr NDZ Municipality's resources.
- 17.2. The ICT Manager shall have the right to block access from within Dr NDZ Municipality's networks to all Internet sites identified as inappropriate. If any user is connected to a site which contains sexually explicit or otherwise offensive material, such user must immediately disconnect from the site concerned.
- 17.3. Dr NDZ Municipality's IT related facilities, and especially its Internet facilities, may not be used knowingly by any official to violate the laws and regulations of the Republic of South Africa or any other nation, or the laws and regulations of any province or municipality.
- 17.4. The use of any municipal resources or illegal activities shall be grounds for the immediate dismissal of the official concerned, and the Council and its officials undertake further to cooperate with any legitimate law enforcement agency in this regard.

- 17.5. No employee may knowingly use Dr NDZ Municipality's IT facilities and resources to download or distribute pirated software or data.
- 17.6. No official may knowingly use the Internet facilities to propagate any malware or malicious code.
- 17.7. No official may knowingly use Dr NDZ Municipality's Internet facilities to disable or overload any computer or network or to circumvent any system intended to protect the privacy or security of another user.
- 17.8. No employee with authorized Internet access may upload any software licensed to DR NDZ Municipality or data owned or licensed to Dr NDZ Municipality without prior authorization of the ICT Manager.
- 17.9. No official may create a communication link requiring dial-out access from any computer which is also connected to the IT network.
- 17.10. No official may use any software which is not provided or approved by the ICT Manager.
- 17.11. Only the IT Manager shall authorize the provision of email addresses to authorized users.

18. Ownership and Classification of Data

- 18.1. Any Municipality data that is created, sent, printed, received or stored on systems owned, leased, administered or authorized by Dr NDZ Municipality is the property of Dr NDZ Municipality and its protection is the responsibility of Dr NDZ Municipality's designated custodians and users.
- 18.2. Data shall be classified as either: Confidential, Sensitive or Public.
- 18.3. **Confidential:** Sensitive data that must be protected from unauthorized disclosure or public release based on local or governmental law (e.g. the Promotion of Access to Information Act, No. 2 of 2000) and other constitutional, statutory, judicial and legal agreements.

Examples of "Confidential" data may include but are not limited to:

18.3.1 Personally Identifiable Information, such as a name in combination with Identification Number (ID) and/or financial account numbers

18.3.2 Employee records

18.3.3 Intellectual Property, such as copyrights, patents and trade secrets

- 18.4. **Sensitive:** Sensitive data that may be subject to disclosure or release under the Promotion of Access to Information Act, No. 2 of 2000, but requires additional levels of protection.

Examples of "Sensitive" data may include but are not limited to:

18.4.1 Operational information

18.4.2 Personnel records

18.4.3 Information security procedures

18.4.4 Research

18.4.5 Internal communications

- 18.5. **Public:** Information intended or required for public release as described in the Promotion of Access to Information Act, No. 2 of 2000. However, any data owned or under the control of the South African Government must comply with the national classification authority and national protection requirements.
- 18.6. Sensitive Information, from the time it is created until the time it is destroyed or declassified must be labelled (marked) with an appropriate information classification designation. Such markings must appear on all manifestations of the information (hardcopies, CD-ROMs, etc.).
- 18.7. Authorized officials who participate in Internet chats and news groups shall refrain from revealing confidential municipal information, client data and any other material covered by existing council policies and municipal procedures with regards to confidential information.
- 18.8. Officials, who release protected information through the Internet whether or not it is inadvertent, could be subject to all the applicable penalties in terms of Dr NDZ Municipality's existing data security policies and procedures.

19. Wireless Security

- 19.1. All wireless Access Points/ Base Stations connected to the Dr NDZ Municipality network must be registered and approved by the ICT Manager.
- 19.2. Access Points/ Base Stations must be subject to periodic penetration tests and audits.
- 19.3. All wireless Network Interface Cards (i.e., PC cards) used in laptop or desktop computers must be registered with the ICTManager.
- 19.4. All access points (APs) must be logically secured to prevent unauthorized access to the AP configuration environment.
- 19.5. AP devices must be configured to only allow pre-defined authorized administrators to make configuration changes.
- 19.6. AP's must be physically secured to protect the AP against physical manipulation.
- 19.7. All wireless LAN access must use Dr NDZ Municipality approved vendor products and security configurations.
- 19.8. All computers with wireless LAN devices must utilize Dr NDZ Municipality approved Virtual Private Network (VPN) configured to prevent all unauthenticated and unencrypted traffic.
- 19.9. Wireless implementations must maintain point to point hardware encryption of at least 56 bits.
- 19.10. Wireless implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.
- 19.11. Wireless implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.
- 19.12. The SSID shall be configured so that it does not contain any identifying information about the Dr NDZ Municipality, such as the Dr NDZ Municipality division title, employee name, or product identifier.

20. Official Website

- 20.1. The **Communications Manager** shall be responsible for the maintenance of Dr NDZ Municipality's website, with the assistance of the **ICT Manager** and the service provider.
- 20.2. Each Director shall ensure that all information required by the Municipal Finance Management Act, as well as any other relevant legislation and Council Policies, is promptly and appropriately submitted to the Communications Manager for display on the official website.
- 20.3. The **Communications Manager** shall (in consultation with the relevant Director) further decide on any other information to be made available on the website.
- 20.4. Only the **Communications Manager** can provide authorization to the service provider, to amend, add and delete information on the official Dr NDZ Municipality website.

21. Protocols

21.1 Reporting Security Incidents

- 21.1.1 If an IT Security incident or breach is suspected or noticed by any employee, then it is the obligation of that employee to immediately notify the ICT Manager.
- 21.1.2 Users are required to note and report any suspected security threats and/or weaknesses in and around IT systems and services.
- 21.1.3 Critically, users must not attempt to prove a suspected weakness within a system, as testing weaknesses might be interpreted as a potential misuse of the system, which could lead to disciplinary action thereafter.
- 21.1.4 The ICT Manager is tasked with the security responsibility of Dr NDZ Municipality and must report all instances of a breach of security, or failure to comply with security measures, or conduct constituting a security risk, as soon as possible to the Chief Directorate Security of the National Intelligence Agency (NIA), and where appropriate to the South African Police Services (SAPS - Crime Prevention Unit) or the South African National Defense Force (SANDF - MI). Where official encryption is concerned, a security breach must also be reported to the South African Communication Security Agency (SACSA).
- 21.1.5 When a breach of security occurs, the existing channels must be used to report it. It is the responsibility of the ICT Manager to ensure that all breaches of security are reported.

21.2 User Names

- 21.2.1 All users must have proper usernames and passwords that will grant them access to the network and network services available for Dr NDZ Municipality.
- 21.2.2 The username and password must be in accordance with the standards as defined in number 10.4.6.10.

On all systems, the standard naming convention incorporates the user's full first name and surname initial (e.g. Joe Blogg's ID would be: Bloggj)

21.2.3 In the case of duplicate user names, the user's name will be placed vice versa of the above to make a user ID unique.

22. PC Support

- 22.1. All support must be performed by the ICT officer. The ICT Manager must be provided with the details of the problem.
- 22.2. All network and PC support calls should be given priority and should be attended to as soon as possible.

23. Disaster Recovery Plan

- 23.1. The ICT Manager, in consultation with the CFO and with the approval of Council, shall enter into such agreements with Dr NDZ Municipality's IT suppliers to ensure that the Municipality's Disaster Recovery Plan is in place, is operational, and is reviewed and tested at least once a year. -
- 23.2. The IT Manager shall prepare, review and update (as circumstances require) a list of persons who must be contacted by users in the event of any disastrous occurrence as set out in the Municipality's Disaster Recovery Plan.
- 23.3. Such lists shall be made available to all authorized users on Dr NDZ Municipality's IT Network.

24. ICT Training and Security Awareness

- 24.1. The ICT Manager is responsible for providing security awareness training, on a periodic basis, to new and existing employees.
- 24.2. Training on applications used by the municipality will be provided to end users by the relevant service provider or ICT Unit.
- 24.3. The Skills Development Officer will facilitate the training between service providers and end users on applications used by the municipality.

25. Acceptance of and Compliance with the ICT Security Controls Policy

- 25.1. Every employee who is allocated the use of any Dr NDZ Municipality IT equipment and/or authorized to access the Internet and/or the Municipality's computer network shall be provided with an email copy of this policy by the ICT Manager.
- 25.2. All employees are required to read through the entire IT Security Controls Policy and then sign the IT Security Compliance Agreement form (see Appendix A) attached to this policy in order to indicate that they have read, understood and accept to comply with this policy accordingly.

26. Policy Violations

- 26.1. Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

27. Policy Review

- 27.1. This policy is subject to annual review or whenever it is deemed necessary by the Municipality, to ensure that it is aligned to prevailing resolutions, regulations and market conditions.

28. Publishing the policy

- 28.1. The policy shall be made available and accessible to all employees through manuals/hard copies.

29. Appendices

- 29.1. Appendix A

RECOMMENDATION

That the report be noted,
That the IT Security Controls Policy as part of the ICT Corporate Governance Framework be approved by Council.

Signature	Aproved by	Date
	S.J. Sondezi	28 may 2026

