



DR NDZ LOCAL MUNICIPALITY

In conjunction with



Symphony PC

ICT Security Policy

Table of Contents

1. Purpose	1
2. Management and staff responsibilities	2
3. Computers	2
4. Network	3
5. Workstations/Notebooks	3
6. Modems	3
7. Offline Media	3
8. Computer Resources	4
9. Access Management	4
10. Passwords	4
11. Authentication	4
12. Time restrictions	5
13. Transaction Logs	5
14. Backup	5
15. Email	5
16. Internet	5
17. Antivirus	6
18. Viruses	6
19. Use of electronic communications and services	6
20. Standards of communication	6
21. Security measures and limitation on access	6
22. Commencement of policy	7
23. Interpretation of the policy	7
24. Permanent/Temporary waiver or suspension of policy	7
25. Compliance and enforcement	7
26. Amendment and abolition of policy	7

1. Purpose

Policy management throughout Kwa Sani local municipality should enforce the following standards:

- a. Establish and maintain management and staff accountability for the protection of information resources.
- b. Promulgate the policy regarding the security of data and information technology resources.
- c. Define the minimum security standards for the protection of information resources.

2. Management and staff responsibilities

Although precautions are taken to safeguard all the systems and data, functional requirements make it impossible to prohibit all access to it. The owner or user of the data must therefore take the necessary precautions to ensure that the integrity, confidentiality and availability of all data, systems and equipment are not compromised. To achieve this the following standards should be adhered to:

- a. Each Departmental Head must see to it that all his or her employees take note of the Policy regarding the implementation and maintenance of data and system security.
- b. Each manager is responsible for assuring an adequate level of security for all the data and resources that form part of his or her component or team.
- c. An employee may only access and or use the information that he or she is authorised to access/use.
- d. No information/images/data that may be offensive to any person, group or organisation may be stored on any of the official computer systems or transported across any official network or system.
- e. As official messages sent via the e-mail system can have a major impact on the image of the municipality, employees should see to it that such messages contain only authorised information and that it is in the format prescribed by the Correspondence and Publication Corporate Standards of the municipality.
- f. All the data and information on the municipality's systems is the property of the office of the municipality. The office retains the right to access any information (e-mail etc.) that is stored on or transported across any of the resources in use and to utilise it for whatever reason it deems necessary.
- g. Employees must report any form of misuse of data, systems and equipment that comes to their attention to their respective managers or the Data Security Manager: IT.

3. Computers

- a. In order to limit exposure to security risks, access to all computer related hardware and other resources must be controlled.
- b. All the domain controllers and all other critical file servers must be kept in a secure (locked) environment and only authorised employees or supervised service representatives should be permitted to enter the room.
- c. Console devices (connected to the servers or domain controllers) must be located in a secure location. Other devices such as external hard disks and tape drives must also be located in secure areas.
- d. Workstations must be kept in a secure environment. Only authorised employees should be allowed to use them.
- e. Printers used to print sensitive documents should be placed in a location not accessible to unauthorised personnel. No sensitive information should be

stored on computers located in an insecure environment.

4. Network

- a. Network devices such as routers, firewall, bridges, hubs and servers should be treated as computers and should be located in a secure environment.
- b. Cables, although less of an immediate security exposure than other computer devices should be placed in either secure or not readily accessible locations.
- c. Employees must not make any unauthorised changes to the physical layout and connection points of the network.

5. Workstations/Notebooks

- a. The workstations / notebooks should not be generally available to nonemployees or unauthorised users.
- b. Sensitive output from printers should either be destroyed or placed in a secure location. If employees work on sensitive information the visual access to the screens should be controlled.
- c. No unauthorised changes may be made to the system configuration of workstations / notebooks.
- d. Employees are not allowed to insert/remove any devices into/from any official workstation / notebook without prior authorisation (E.g. Processors, memory modules, controller cards etc.)
- e. Employees are not allowed to install any program on any official computer / workstation without the prior authorisation. No sensitive or classified information should be stored on workstations / notebooks that are not located in a secure environment.
- f. Please note that data stored on workstations is not secured through the normal network security measures and the necessary precautions to safeguard such data should be taken. Should the current local workstation / notebook security be of any concern, additional measures can be instituted. The Centre Manager: IT can be contacted in this regard.

6. Modems

No modems and or related devices may be attached to and or used on any official telephone line, computer, workstation and or network device without prior authorisation.

7. Offline media

Backup media (e.g. tapes, disks or CD?s) must be secured against unauthorised use and tampering.

8. Computer Resources

- a. Critical systems (servers, domain controllers, network equipment and workstations) should be provided with an uninterrupted power supply (UPS).
- b. The operation and functionality of UPS's must be tested regularly according to prescribed testing procedures.
- c. Smoking is not allowed in areas containing computer equipment.
Unauthorised access to the computer and network related resources are not allowed.

9. Access management

- a. Every account must have an owner. (Someone who is responsible for account usage, password changes etc.)
- b. A record should be maintained showing each user's profile. All modifications to user accounts should be recorded.
- c. A new user may be registered on the system by submitting a written application with a list of services, programs and or data to which access is required. This application has to be recommended by the applicant's supervisor and approved by the relevant Manager. After approval has been granted, the network administrator/s will register the new user.

10. Passwords

- a. Passwords are required to gain access to all the domain controllers and file servers. No one will be allowed to access any system without a valid password.
- b. Users will be forced to change passwords on the domains and servers every 30 days.
- c. Passwords will be encrypted by the system.
- d. The minimum password length is set to eight characters and must contain alpha as well numerical characters.
- e. Care should be taken that passwords are not easily guessed (E.g. names, month etc.)
- f. The use of a screensaver password is recommended.
- g. Users will be allowed three login attempts before the account will be locked. This lock will remain in effect for three months or until opened by the Network administrator.
- h. Previously used passwords are not allowed.
- i. Passwords that expire must be changed immediately.

11. Authentication

Critical systems (such as SAMRAS) may require further authentication by means of user log-on (USER-ID and password) to the applicable system. The specific system

administrator must control this.

12. Time Restrictions

Time restrictions are set on the domain controllers and file servers that carry the HR, Financial and other critical information. All the users will be granted access from 07:00 to 18:00 from Monday to Friday. Exceptions to the above will only be allowed with prior authorisation from the Municipal Manager.

13. Transaction Logs

The domain controller and file server error logs must be followed up regularly by the network administrator. All transaction logs must be followed up regularly by the network administrator.

14. Backup

- a. It is the responsibility of the specific user to ensure that his/her data is backed up regularly. Files containing static information should be protected from unauthorised modification.
- b. Critical applications and or data files should be backed up and stored off-site. The location and procedure to access the files must be available to the specific manager.
- c. The Data Security Manager must ensure that the approved corporate backup procedures are followed.

15. Email

- a. The official e-mail system may not be misused for private purposes. Electronic mail messages are not encrypted and the e-mail system can therefore not be used to transmit sensitive and/or classified material.
- b. The Office retains the right to access and monitor any information sent via the e-mail system. No private information/images/data that may be offensive to any person, group or organisation may be sent to any destination via the official e-mail system.
- c. As messages sent via the official e-mail system can have a major impact on the image of the Office, employees must see to it that such messages contain only authorised information and that it is in the format prescribed by the Correspondence and Publication Corporate Standards of the Office.

16. Internet

- a. The connection of any Office network to an external network (INTERNET) must be protected by appropriate security measures (e.g. firewall restrictions etc.). Internet access is provided on a limited basis for research and communication purposes only. The procedures set out in paragraph

(application and authorisation) must be followed to gain access to this service. No material that may be deemed offensive may be downloaded through the official systems and networks.

- b. Due to bandwidth constraints no live streaming of video and or audio signals over the Internet will be allowed.

17. Antivirus

Kwa Sani local municipality will use a single anti-virus product for antivirus protection and that product is ESET NOD32 Antivirus. The anti-virus product is operated in real time on all servers and client computers. The Antivirus is configured for real time protection.

- a. The anti-virus library definitions shall be updated at least once per day.
- b. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

18. Viruses

Users should take care not to distribute virus infected documents, programs and or data through the network or e-mail system. All workstations/notebooks etc. should be regularly scanned for possible virus infections.

The official antivirus software should be installed on all the computers in use in the Municipalities.

All instances of virus infections should be reported. All diskettes should be scanned for possible viruses before any programs on it are executed or any data files are read or printed. Users will be informed of antivirus software updates via e-mail.

19. Use of electronic communications and services

Employees are allowed access to communication facilities and services for bona fide business purposes.

20. Standards of communication

- a. Each user has a responsibility to use the communication facilities and services in a lawful, informed and responsible way and in a manner that conforms to computer network etiquette, custom, courtesy and corporate policy.
- b. Users should apply exactly the same standards of care and professionalism when using electronic communication facilities and services as they would apply in any other business related communications.

21. Security measures and limitations on access

Each user must comply with all of the Municipality's access procedures, including the

use of assigned user ID's and use of the licensed software made available to the employee by the Municipality. User ID's may not be shared with other persons, a user may not use email accounts assigned to other individuals to send or retrieve messages. It remains the responsibility of each user to safeguard their passwords to prevent unauthorised access. Every user must ensure that system access is signed off when they leave their desk

22. Commencement of the policy

The policy will come into effect on the date of adoption by council.

23. Interpretation of the policy

- a. All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise. Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
- b. The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
- c. If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

24. Permanent/Temporary waiver or suspension of policy

- a. This policy may be partly or wholly waived or suspended by the Municipal Council on temporary or permanent basis.

Notwithstanding clause No. 17 the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council.

25. Compliance and enforcement

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

26. Amendment and abolition of policy

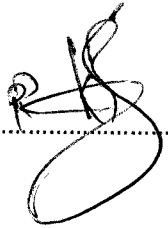
- a. This policy may be amended or repealed by the council as it may deem necessary.

27. COUNCIL APPROVAL AND EFFECTIVE DATE

Approval of Policy by Council and Effective date: 06/06/2017

MUNICIPAL MANAGER

DATE



.....

19/06/2017