



DR NKOSAZANA DLAMINI ZUMA LOCAL MUNICIPALITY

CYBER SECURITY POLICY

Contents

Document Control	2
1. Preamble	5
2. Purpose	6
3. Problem Statement for Dr. Nkosazana Dlamini Zuma Local Municipality	6
4. Summary	8
5. Account Management for Dr. Nkosazana Dlamini Zuma Local Municipality	8
6. Change Management	10
7. Security Monitoring	11
8. Security Awareness and Training	12
9. Vendor Access / Third Party Access	14
10. Non-Disclosure of Client Information	16
11. Safeguarding and Disposal of Client Information Safeguarding	17
12. Review and Respond	18
13. Device Security	19
14. Email Security	20
15. Transferring Data.	21
16. Disciplinary Action	22
17. Policy Monitoring and Evaluation	23
18. COMMENCEMENT OF THIS POLICY	24
19. INTERPRETATION OF THIS POLICY	24
20. PERMANENT/TEMPORARY WAIVER OR SUSPENSION OF THIS POLICY	25
21. AMENDMENT AND/OR ABOLITION OF THIS POLICY	26
22. COMPLIANCE AND ENFORCEMENT	27

1. Preamble

The potential for data theft, fraudulent activities, and security breaches poses significant threats to a municipality's systems, technology infrastructure, and reputation. Therefore, Dr Nkosazana Dlamini Zuma Local Municipality has developed this policy to delineate the security protocols implemented to safeguard information and maintain its integrity.

The management of the municipality has demonstrated effective leadership and a strong commitment to information security. They have actively supported the development of a cyber-security policy, ensuring its creation and implementation. This document outlines the necessary safeguards and controls aimed at protecting information and aligning with the municipality's strategic goals.

To enhance the Nkosazana Dlamini Zuma Local Municipality's information security program, the following measures must be taken:

- **Designate Coordinators:** Appoint one or more employees to oversee and coordinate the information security program.
- **Risk Identification and Assessment:** Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of DR NDZ information. Assess the adequacy of existing safeguards to manage these risks.
- **Safeguard Implementation and Monitoring:** Develop and implement appropriate safeguards to address identified risks. Regularly monitor and test the effectiveness of these safeguards.
- **Service Provider Management:** Choose and retain service providers who can uphold suitable safeguards for the information. Ensure these providers are contractually obligated to implement and maintain these safeguards.
- **Program Adjustment:** Continuously review and adjust the information security program to account for any significant changes or developments that may impact its effectiveness.

b. Information Technology and Information

i. Confidentiality

Information varies in its level of confidentiality, and for each level, the owner may restrict access to specific individuals. Information technology (IT) systems are employed to protect the confidentiality of municipal information, ensuring that unauthorized individuals cannot access it.

ii. Integrity

Regardless of its confidentiality, all information must be safeguarded against unauthorized changes. Users must have confidence in the information they receive, knowing it is reliable, trustworthy, and has not been altered without their knowledge. IT systems play a crucial role in maintaining the integrity of information by preventing unauthorized changes. When authorized changes occur, the details (nature of change, date and time, system, user) must be recorded.

iii. Availability

Municipal information must be accessible to authorized users whenever needed. IT systems ensure that information is readily available and provide reliable and robust means for users to access and work with it. Ensuring availability involves maintaining reliable IT infrastructure to support uninterrupted access to necessary information.

By addressing these areas—confidentiality, integrity, and availability—the municipality can effectively protect its information assets and ensure their proper use and management.

f. Inactive New User Accounts

- New user accounts that have not been accessed within 30 days of creation will be disabled to ensure they are not improperly used.

g. Responsibilities of System Administrators and Designated Staff

- **Account Creation:** System Administrators or designated staff are responsible for creating user accounts.
- **Account Removal:** They must remove accounts of individuals who change roles within the municipality or are no longer associated with it.
- **Account Modification:** A documented process must be in place to modify user accounts for situations such as name changes, accounting changes, and permission adjustments.
- **Periodic Review:** A documented process for periodically reviewing existing accounts to ensure their validity must be maintained.
- **Independent Audit:** System Administrators are subject to independent audit reviews to verify compliance.
- **Account Listings:** They must provide a list of accounts for the systems they administer when requested by authorized DR NDZLM management.
- **Security Incident Cooperation:** System Administrators must cooperate with authorized DR NDZLM management during security incident investigations.

g. Change Management Log

- A Change Management Log must be maintained for all changes. The log must include, but is not limited to:
 - Date of submission and date of change
 - Owner contact information
 - Nature of the change

h. Compliance with Change Management Process

- All information systems must adhere to a change management process that meets the standards outlined above.

7. Security Monitoring

a. Real-Time Monitoring with Automated Tools

- Automated tools will provide real-time notifications of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed, and the tools will report exceptions. These tools will be deployed to monitor:
 - Internet traffic
 - Email traffic
 - Local Area Network (LAN) traffic, protocols, and device inventory
 - Operating system security parameters

b. Regular Log and File Monitoring

- The following logs and files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk assessment:
 - Automated intrusion detection system logs
 - Firewall logs
 - User account logs
 - Network scanning logs
 - System error logs
 - Application logs
 - Data backup and recovery logs
 - Help desk trouble tickets
 - Telephone activity - Call Detail Reports
 - Network printer and fax logs

e. Responsibility of Information and System Owners

- Information and system owners must ensure that all administrators receive the appropriate training and knowledge required to deliver effective service across all Dr Nkosazana Dlamini Zuma Local Municipality business areas. Additionally, they are responsible for ensuring administrators have the necessary knowledge to effectively protect information assets.

f. Regular Information Security Education and Training

- The DR NDZLM Human Resources Management department, in collaboration with the ICT department, must conduct regular information security education and training sessions. These sessions ensure that users are continually aware of and updated on cybersecurity policies, threats, and concerns.

8.1 New Employees

To mitigate the risk of unintentional disclosure of confidential information by employees, the Human Resources department will ensure that newly onboarded employees are referred to this policy. New employees will be required to formally acknowledge that they have read, understood, and will adhere to the policies outlined herein. This acknowledgment serves to reinforce the importance of confidentiality and the responsibilities associated with handling sensitive information within Dr. Nkosazana Dlamini Zuma Local Municipality.

8.2 Existing Employees

To mitigate the risk of unintentional disclosure of confidential information by employees, cyber security training and awareness sessions will be provided as an integral part of employee onboarding and ongoing development. Additionally, existing employees will be required to acknowledge this policy, demonstrate understanding of its contents, and agree to apply it. This acknowledgment will be included in the annual sign-off process, along with the code of conduct, reaffirming employees' commitment to upholding security standards within Dr. Nkosazana Dlamini Zuma Local Municipality.

d. Employee List Submission

- Each vendor must provide Dr Nkosazana Dlamini Zuma Local Municipality with an updated list of all employees working on the contract within 24 hours of any staff changes.

e. Identification Badge Requirement

- On-site vendor employees must obtain and display a Dr Nkosazana Dlamini Zuma Local Municipality identification badge at all times while on Municipality premises. Badges must be returned upon contract completion or employee departure.

f. Clearance for Sensitive Information

- Vendor employees with access to sensitive Municipality information must be cleared to handle such information.

g. Additional Contractual Details

- Various additional contractual details include following Municipality change control processes, defining work parameters and hours, maintaining disabled vendor accounts except when in use for authorized maintenance, and maintaining logs of major work activities.

h. Secure Information Handling Upon Departure

- Vendors must ensure that all sensitive information is collected and returned to Dr Nkosazana Dlamini Zuma Local Municipality or destroyed within 24 hours of a vendor employee's departure from the contract.

i. Return or Destruction of Municipality Property

- Upon contract termination or at the Municipality's request, the vendor must return or destroy all Municipality property and provide written certification of the return or destruction within 24 hours.

j. Surrender of Identification Badges and Equipment

- Upon contract termination or at the Municipality's request, the vendor must surrender all Dr Nkosazana Dlamini Zuma Local Municipality identification badges, access cards, equipment, and supplies immediately.

k. Software Inventory and Licensing

- All software used by the vendor in providing services to Dr Nkosazana Dlamini Zuma Local Municipality must be properly inventoried and licensed.

11. Safeguarding and Disposal of Client Information Safeguarding

Safeguarding

The Municipality restricts access to client information to employees who need such information to provide services. Authorized employees, known as Record Managers, must secure client information daily, storing it in a secure compartment or receptacle at the close of business. Electronic files containing client information must be password-protected and firewall-protected against unauthorized access. Conversations involving client information must be conducted privately to prevent unauthorized persons from overhearing or intercepting them.

Safeguarding standards apply to all aspects of the municipality affecting security, including computer security, physical security, and personnel procedures. Key safeguarding standards adopted by the municipality include:

- **Access Controls:** Implement controls to authenticate and permit access only to authorized individuals. Record Managers must prevent employees from providing client information to unauthorized persons who may attempt to obtain it fraudulently (e.g., requiring the use of user IDs and passwords).
- **Physical Access Restrictions:** Limit access to physical locations containing client information, such as buildings, computer facilities, and records storage facilities, to authorized individuals only (e.g., using intruder detection devices and fire- and burglar-resistant storage devices).
- **Encryption:** Encrypt electronic client information both in transit and in storage on networks or systems to which unauthorized individuals may have access.
- **System Modifications:** Ensure that modifications to customer information systems are consistent with the municipality's information security program through independent approval and periodic audits.
- **Procedures for Access Control:** Implement dual control procedures, segregation of duties, and background checks for employees with responsibilities for or access to client information (e.g., having data entry reviewed for accuracy by personnel not involved in its preparation, and having adjustments to master records reviewed and approved by personnel other than those approving routine transactions).
- **Cyber Security Compliance:** Ensure that all mobile and computing devices connecting to applications or resources used by the municipality comply with the Cyber Security Policy.

- **Reporting and Documentation:** Documenting the findings of each assessment and the steps taken to address identified vulnerabilities, ensuring a clear record of actions for accountability and future reference.

13. Device Security

a. Municipality Use

To ensure the security of all municipality-issued devices and information, Dr Nkosazana Dlamini Zuma Local Municipality employees are required to:

- **Password Protection:** Keep all municipality-issued devices, including tablets, computers, and mobile devices, password-protected with a minimum of 8 characters.
- **Device Security:** Secure all relevant devices before leaving their desks.
- **Authorization for Removal:** Obtain authorization from the Office Manager and/or Inventory Manager before removing devices from municipality premises.
- **Password Confidentiality:** Refrain from sharing private passwords with coworkers, personal acquaintances, and senior personnel.
- **Software Updates:** Regularly update devices with the latest security software.

b. Personal Use

Dr Nkosazana Dlamini Zuma Local Municipality recognizes that employees may need to use personal devices to access municipality systems. In these cases, employees must report this usage to management for record-keeping purposes. To ensure municipality systems are protected, all employees are required to:

- **Password Protection:** Keep all personal devices password-protected with a minimum of 8 characters.
- **Device Security:** Ensure all personal devices used to access municipality-related systems are password-protected.
- **Antivirus Software:** Install full-featured antivirus software and regularly upgrade it.
- **Device Locking:** Lock all devices if left unattended.
- **Continuous Protection:** Ensure all devices are protected at all times.
- **Network Security:** Always use secure and private networks.

- **Enable Two-Factor Authentication:** Implement two-factor authentication (2FA) on email accounts to add an extra layer of security.
- **Regular Training:** Participate in regular cybersecurity training sessions to stay updated on the latest email security threats and best practices.
- **Email Encryption:** Use email encryption tools for sensitive communications to prevent unauthorized access.
- **Update Email Software:** Keep email clients and related software up-to-date with the latest security patches and updates.
- **Monitor for Phishing:** Be vigilant for common phishing tactics and familiarize yourself with the signs of a phishing attempt.
- **Secure Networks:** Always access email accounts over secure, private networks rather than public Wi-Fi to reduce the risk of interception.

15. Transferring Data.

Dr Nkosazana Dlamini Zuma Local Municipality recognizes the security risks associated with transferring confidential data both internally and externally.

To minimize the risk of data theft, all employees are required to follow these guidelines:

- **Restrict Transfers:** Avoid transferring classified information to unauthorized employees and external parties.
- **Use Secure Networks:** Only transfer confidential data over the municipality's secure networks.
- **Obtain Authorization:** Secure the necessary authorization from senior management before transferring any confidential data.
- **Verify Recipients:** Confirm the identity of the recipient and ensure they have the appropriate security measures in place to handle the data securely.
- **Adhere to Laws and Agreements:** Comply with the municipality's data protection laws and confidentiality agreements during all data transfer processes.
- **Report Incidents:** Immediately notify the ICT Unit of any data breaches, encounters with malicious software, or suspected scams.

Additional Disciplinary Measures

To ensure clarity and consistency in disciplinary actions, the following measures are also in place:

- **Documentation:** All disciplinary actions will be documented, including the nature of the violation, the steps taken in response, and any communications with the employee.
- **Escalation Protocols:** For severe violations, the matter may be escalated to higher management or legal counsel to determine appropriate actions.
- **Training and Awareness:** Employees will be provided with regular training and resources to understand the policy and the implications of non-compliance.
- **Appeal Process:** Employees will have the right to appeal disciplinary actions if they believe they have been unjustly penalized. Appeals will be reviewed by an independent committee.
- **Rehabilitation:** Where appropriate, employees may be given the opportunity to undergo further training or corrective programs to address and rectify their behaviour.

17. Policy Monitoring and Evaluation

a. Policy Audit

The Internal Audit team must conduct periodic audits of policy implementation to track and assess compliance. These audits ensure that all aspects of the policy are being adhered to and identify areas for improvement.

b. Policy Review

This policy shall be reviewed annually, coinciding with the financial year, by the Information Security Management Team. This review will consider any changes in the regulatory environment, emerging threats, and feedback from the audits to update and enhance the policy as necessary.

Additional Measures for Effective Monitoring and Evaluation

To ensure the ongoing effectiveness of this policy, the following measures will also be implemented:

b. Dispute Declaration

Any dispute regarding the interpretation of this policy must be declared in writing by the concerned party.

c. Final Interpretation

The Municipal Manager shall provide the final interpretation of this policy in the event of a written dispute.

d. Further Dispute Resolution

If the concerned party is not satisfied with the Municipal Manager's interpretation, the dispute may be escalated to the South African Local Government Bargaining Council or Arbitration for further resolution.

Additional Details for Clarity

- **Definitions Section:** Consider adding a definitions section to the policy to clarify any terms that might be open to interpretation.
- **Dispute Resolution Process:** Clearly outline the steps and timelines for the dispute resolution process to ensure transparency and efficiency.
- **Communication:** Ensure that all employees are aware of the procedures for disputing the interpretation of the policy and their rights within this process.
 - **Documentation:** Maintain thorough records of all disputes and interpretations to provide a reference for future cases and to ensure consistency in the application of the policy.

20. PERMANENT/TEMPORARY WAIVER OR SUSPENSION OF THIS POLICY

a. Council Approval

This policy may be partially or fully waived or suspended by the Municipal Council on either a temporary or permanent basis. Such decisions shall be made following consultation with Management and Trade Unions.

b. Emergency Circumstances

In exceptional circumstances of emergency, the Municipal Manager may temporarily waive or suspend this policy. However, such actions must be reported to the Council and Trade Unions promptly, notwithstanding clause No. 10.1.

22. COMPLIANCE AND ENFORCEMENT

a. Disciplinary Action for Violation

Any violation or non-compliance with this policy will warrant disciplinary action.

b. Responsibility for Enforcement

It is the duty of all Managers, Supervisors, members of the Executive Committee, and Council to ensure adherence to this policy and enforce compliance effectively.

Additional Measures for Effective Compliance and Enforcement:

- **Training and Education:** Provide comprehensive training and education sessions to all employees to ensure they understand the policy requirements and consequences of non-compliance.
- **Regular Audits:** Conduct regular audits and assessments to monitor compliance levels and identify areas needing improvement.
- **Accountability:** Hold individuals accountable for enforcing compliance within their respective departments or teams.
- **Rewards and Recognition:** Establish a system for recognizing and rewarding compliance with the policy to incentivize adherence.
- **Feedback Mechanism:** Encourage employees to provide feedback and suggestions for improving compliance procedures and enforcement mechanisms.

By implementing these measures, Dr Nkosazana Dlamini Zuma Local Municipality ensures that its policies are effectively enforced, promoting a culture of compliance and accountability among its employees.

Signature	Approved by	Date
	S.J. Soudani	28 May 2026