

DRAFT

I.T NETWORK SECURITY POLICY

NDLAMBE MUNICIPALITY



Ndlambe IT Network Security Policy

	<u>Contents</u>	<u>Page</u>
1	PURPOSE	3
2	BACKGROUND	3
3	SCOPE	3
4	TERMINOLOGY	3
5	POLICY	4
5.1	General Policy Requirement	4
5.1.1	Authentication	4
5.1.2	Logical Access Control	5
5.1.3	Privacy / Confidentiality	5
5.1.4	Integrity	5
5.1.5	Audit Logging / Accountability	5
5.1.6	Availability	5
5.2	Network Management	5
5.3	Traffic Management	6
5.4	Network Operations	7
5.5	Risk Management	8
6	REPORTING	8
7	SUMMARY OF MAIN RESPONSIBILITIES	8
8	DISCIPLINARY CODE OF PRACTICE	10
9	EFFECTIVE DATE	10

1 PURPOSE

The purpose of this policy is to provide a solid foundation for the development, implementation and maintenance of secure practice within NDLAMBE Municipality's networking environment.

2 BACKGROUND

Network security involves the protection of the municipality from the threats posed by authorised and unauthorised network activity. The threat(s) increases due to the interconnectivity of networks and the convergence of different network services (voice, data etc), making it difficult to draw boundaries around the municipality and to apply controls for the protection of the internal assets.

There are obvious dangers that external connections may increase the risk of a security compromise, whilst being unaware of the risk. Network connections should therefore be protected at a level based on the risk. The assumption must be that connecting parties are to a certain degree hostile and have to be strictly controlled to ensure that the access, for which the connection was agreed, is maintained.

3 SCOPE

This policy applies to all network administrators, technical and maintenance personnel, designers, users and the owner of the municipality's network. The network security policy is considered as part of the municipality's Security Policy.

4 TERMINOLOGY

For the purposes of this policy the following terminologies apply:

Information Security. Information Security encompasses the management processes, technology and assurance mechanisms that will allow the municipality to trust their transactions, the information is usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and that confidential information is withheld from those who should not have access to it.

Network Security. The protection of networks and their services from unauthorised modification, destruction or disclosure and providing the assurance that the network performs its critical functions correctly.

Network Device. Any information technology and communication device used to form the infrastructure required for communication services (servers, routers, switches, bridges, firewalls, encryption devices).

De-Militarised Zone (DMZ). The frontline when protecting valuables (i.e. information assets) from direct exposure to an un trusted environment, or; a network added between a protected network and an external network in order to provide an additional layer of security.

Sensitive Information. Any information that, if disclosed without appropriate authorisation, will compromise the municipality's security or business initiatives.

Network Sniffing. The use of hardware and/or software mechanisms to analyse / monitor electronic communications (traffic) over a network.

Operational Environment. The environment responsible for the implementation and maintenance of the day-to-day security activities.

Communication Carrier. The infrastructure provided by a service provider (e.g. TELKOM) to interconnect communication devices.

Computer Network. A range of computers connected by means of communication carriers.

Data Traffic. Information in electronic format, which is communicated over a communications carrier.

Access. Physical or logical access to information or information systems through a range of network devices.

5 POLICY

5.1 General Policy Requirement

It is the policy of the municipality to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information. As a minimum, authentication, access control, privacy (confidentiality), integrity, availability and audit logging must be implemented as security services on the municipality's network.

5.1.1 Authentication

All network devices, management stations and network users / administrators must have unique identifiers in accordance to a defined

naming convention. Passwords must be implemented in accordance with the municipality's password standards.

5.1.2 Logical Access Control

Access control mechanisms must be implemented on all network devices and management systems. Access may only be granted in line with the job responsibilities of network administrators (based on the "need-to-have" principle). External access to network devices and management systems must be restricted to the minimum and where applicable, strict control mechanisms must be implemented.

5.1.3 Privacy / Confidentiality

All reasonable measures must be taken to ensure that internal and external communications between networks and network devices as well as client interfaces may not compromise security. Where applicable, encryption mechanisms must be implemented.

5.1.4 Integrity

Mechanisms / procedures must be in place to ensure the integrity of all network devices and traffic. Real time alerts should be generated for all configuration / permission changes that can lead to a breach in security.

5.1.5 Audit Logging / Accountability

Audit information, including alerts generated for failed logon attempts, must be available for all network devices and management systems.

5.1.6 Availability

Network(s) and network services must be available as and when required and capable of handling the network traffic requirements.

5.2 Network Management

1. The manager responsible for Information Technology must assign overall responsibility for network activity and appoint a network owner. It is the responsibility of the network owner to, among others, ensure compliance with this policy and to provide monthly feedback with regard to the state of compliance as part of the municipality's information security risk management process.
2. Network strategy, standards, principles, guidelines, architectures, procedures, design, configuration, equipment, software, inventories and cabling information must be formally documented, kept up to date and

reviewed annually. Only authorised personnel may be allowed access to this information / documentation in accordance with the sensitivity / security classification.

3. Human resources and infrastructure that are critical to the continuity of network services should be identified and single points of failure must be minimised.
4. All external connections to the municipality's network must be preceded with a risk analysis and at a minimum be protected by a firewall or similar type of device. Non IP network connections must be secured by definition characteristics and / or specific configurations to restrict access capabilities and to meet the security requirements. The connections must be reviewed periodically via a traceable process. Where applicable, internal networks (i.e. LAN's), where sensitive information is processed, must also be protected commensurate to its sensitivity.
5. All external connections / third parties to the network should be assigned an owner, approved by the network owner and the head of the business unit, individually identified and recorded. (Please refer to the detailed policy on third party connections).
6. In order to provide a clear picture of the network and to minimise unwanted connections, network access control must be centrally approved by the network owner or a responsible person as appointed by him/her.
7. The municipality's network should preferably be protected by creating a DMZ. No sensitive information may be stored in the DMZ.
8. Services obtained from internal or external service providers must be defined in formal agreements. The agreements must specify the requirements for security controls. Mechanisms must be in place to measure adherence to these requirements.
9. Only network services required specifically for business purposes are allowed and all unnecessary network services must be disabled.
10. Formal set-up standards must be agreed too and no network device may be deployed in the operational environment with default / factory password settings or any other configuration that poses a threat to security for example open FTP ports or broadcasting configuration information over the network.
11. Formal processes must be implemented to ensure that all applicable security patches are kept updated.
12. Methods and procedures must be implemented whereby network security issues are dealt with in a consistent manner. The results must be archived for future reference purposes.

5.3 Traffic Management

1. Network devices must be configured to prevent unauthorised access. The configuration(s) must be reviewed at least annually or after significant changes and health checked at least once every quarter. Unauthorised changes must be handled as a breach of security.

2. With the exception of pre-approved operational network sniffing or monitoring devices, no other network sniffing or monitoring devices may be installed / activated without the explicit authorisation of the Manager for IT.
3. Measures must be implemented to ensure the network filtering devices cannot be bypassed and can only be accessed from designated workstations or specified IP addresses via authorised secure channels (for example SSL).
4. Divulgence / broadcast of information about the network must be restricted to the absolute minimum.
5. Traffic flowing over the network must be afforded the same protection / security characteristics as when stored in accordance with the classifications of the information.

5.4 Network Operations

1. Service levels between service providers and the municipality must be agreed too and continuously and formally monitored to ensure an acceptable level of service. All unusual entries / activities must be investigated and reported to appropriate line management for corrective action.
2. Pre authorised intrusion detection mechanisms should be employed as protection against possible attacks (depending of budget and availability of technical skills) .
3. Effective incident response, business continuity and disaster recovery planning processes must be implemented.
4. Network changes must be documented, formally accepted by the network owner and follow an accepted IT change management policy and standard.
5. Physical access to network devices must be restricted to authorised personnel. Service providers and / or contractors with no service record / history, must remain under constant observation when allowed access to restricted areas.
6. To reduce the risk of data in transit being intercepted, special care must be taken to protect network cables from tampering or disruption.
7. Back-up versions of essential network information and software (including communications software and utilities, network control tables / settings, configuration diagrams and inventories and device configurations) must be taken at such intervals required for the continued availability of the network. The back-ups should be protected from loss, damage and unauthorised access by storage in a fireproof safe on-site and copies off-site.
8. Remote maintenance must be controlled by restricting access rights and logging all activity. Diagnostic ports on network equipment must be protected by access controls.
9. Access to network devices that are primarily used for security services must be approved by the I.T Manager. Access to any other network

devices must be regulated via a formal process to request and authorise access. Record must be kept regarding the authorised access and a process implemented to ensure the timorous revocation of redundant access. The controls must be in the form of formal and traceable processes.

10. Internal or external remote maintenance sessions to devices that form the security barrier (the security objects used for protection) may not be allowed unless protected / controlled through a secure channel (e.g. SSL for Telnet)
11. No modems may be connected to the network without the prior approval of the applicant's manager and the Manager responsible for IT. A register of all approved modems must be maintained.
12. No user may simultaneously be connected to another network by using a modem while still connected to the municipality's network.

5.5 Risk Management

1. A formal risk analysis must be carried out at least annually for networks that support critical business applications. The results of risk analysis must include a clear indication of key risks, an assessment of their potential business impact and recommendations for the actions required to reduce risk to an acceptable level.
2. The security status of the network must be subject to thorough, independent and regular security audit / review. Agreed recommendations from security audits / reviews should be implemented and reported to top management.
3. With the exception of Internal Audit, no unauthorised or clandestine audit or risk analysis may be conducted without the prior approval of the network owner.
4. A risk analysis must be done and the results formally considered before the implementation of technology that could negatively affect the security of the network. (The introduction of wireless networks serves as an example).
5. A process must be implemented to ensure compliance with new or existing local and international statutory requirements.

6 REPORTING

Unless specifically and formally approved by the Manager responsible for IT, any deviation from this policy is strictly prohibited.

7 SUMMARY OF MAIN RESPONSIBILITIES

Following is a summary of the main responsibilities as derived from the policy document:

Responsibility		
	I.T.MANAGER	INTERNAL AUDIT
Formulate Network Strategy	✓	
Implementation of policy	✓	
Awareness	✓	
Policy Update / Revision	✓	
Compliance Monitoring	✓	
Monitor Reports	✓	
Management Information	✓	
Reporting of Security Incidents	✓	
Formulation of Operational Processes	✓	
Formulation of Technical Network Standards	✓	
Risk Analysis	✓	
Centralised Access Control	✓	
Network Inventory	✓	
Network Security Device Management	✓	
Approval of Third Party Connections	✓	
Network Contingency Planning (including disaster recovery)	✓	
Compliance reviews from a management perspective	✓	
Independent ad hoc review		✓

8 DISCIPLINARY CODE OF PRACTICE

The municipality views the implementation of this policy in a serious light and will not hesitate to act against violators. Non-compliance to this policy is grounds for disciplinary actions up to and including summary dismissal.

9 EFFECTIVE DATE

This policy comes into effect on date of approval.

Implementation Date	Revision Date

Document Control Sheet

NDLAMBE MUNICIPALITY

NETWORK SECURITY POLICY

Document Title: NDLAMBE Municipality I T Data and Systems Security Policy

Department **Document Number** **Revision**

Issue Date