



I.T DATA AND SYSTEMS SECURITY POLICY

Contents

- 1 PREAMBLE
- 2 PURPOSE OF THE POLICY
- 3 SCOPE
- 4 GENERAL GUIDELINES
- 5 INFORMATION SECURITY DEFINITIONS
- 6 HIGH LEVEL INFORMATION SECURITY PRINCIPLES
 - 6.1 Protection
 - 6.2 Risk Management
 - 6.3 Information Management
 - 6.4 Co-operation
 - 6.5 Organisation
 - 6.6 Privacy
 - 6.7 Third Parties
- 7 GENERALLY APPLICABLE POLICIES
 - 7.1 Classification
 - 7.2 Confidentiality
 - 7.3 Availability
 - 7.4 Integrity
 - 7.5 Non-Repudiation
 - 7.6 Accountability
 - 7.7 Access Control
 - 7.8 Authentication
 - 7.9 Reporting of Security Incidents
 - 7.10 Exceptions
- 8 MANAGEMENT POLICY
 - 8.1 General Requirements
 - 8.2 Authentication Requirements
 - 8.3 Clear Screen and Clear Desk Policy
 - 8.4 Passwords
 - 8.5 Access Control Policy
 - 8.6 Virus Protection
 - 8.7 Account Policies
 - 8.7.1 Password
 - 8.7.2 Account Lockout Policy
 - 8.7.3 General
 - 8.8 Local Policies
 - 8.8.1 Audit Policy
 - 8.9 Security Options
- 9 USER POLICY
- 10 LEGAL AND REGULATORY REQUIREMENTS
- 11 DISCIPLINARY CODE OF PRACTISE
- 12 IMPLEMENTATION PLAN
- 13 EFFECTIVE DATE
- 14 COMPLIANCE AGREEMENT



1. PREAMBLE

Information and information systems are critical and vitally important to the municipality. Without reliable information the municipality could be adversely affected, both financially and reputation wise. Therefore, this policy states the minimum requirements and the responsibility that all employees, temporaries, contractors and management must comply with in order to secure the municipality's information.

This policy sets out the approach taken to manage information security to ensure that information assets are properly protected against a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accident

NDLAMBE Municipality (NDLAMBE) management has a duty to preserve, improve, and account for all information and information systems. They must additionally make sure that information assets are protected in a manner that is at least as secure as other organisations in the same industry handling the same type of information. To achieve this objective, annual reviews of the risks to NDLAMBE's information assets will be conducted. Similarly, whenever a security incident or audit finding indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce the municipality's exposure.

The municipality's information must be protected in a manner appropriate to its sensitivity, value, and credibility. Security measures are therefore used regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. This protection includes restricting access to information based on the need-to-know principle.

Decision-making within the municipality is also critically dependent on information, as management need to be able to rely on the integrity of information in terms of accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc the awareness of and fine-tuning of such information is an important information management activity. Information security requires the participation and support from all staff (including consultants, contractors, and temporaries) who will be provided with sufficient training and supporting procedures / policies to allow them to properly protect and manage the municipality's information assets. It is the responsibility of all municipal staff to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats observed or suspected to systems or services to the IT manager responsible for information/system security as soon as possible to enable the volumes and costs of incidents and malfunctions to be quantified and monitored.

2. PURPOSE OF THE POLICY

This document defines the policy of NDLAMBE for the application of information Security to protect the municipality's corporate information, information systems and applications against all threats, which could endanger their confidentiality, integrity and availability.

The objective of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. The purpose of this Policy is to protect the municipality's information assets in terms of Confidentiality, Integrity and Availability.



3. SCOPE

This policy applies to all offices and users of information within NDLAMBE. It applies across hardware platforms, to all departments, business units and to all partners, staff and contractors of the municipality.

4. GENERAL GUIDELINES

All managers within the municipal departments are responsible for ensuring that personnel receive and understand the IT policy of the Department. Staff are required to sign a confidentiality and security undertaking. Clients and stakeholders that access the municipality's facilities are required to sign Security Undertakings accepting the conditions as set out in this policy. The management of the network rests with the IT section and can involve third party contractors as a service provider for the municipality. Where this is so, the service provider must sign a Security and Confidentiality undertaking accepting the guidelines and rules as set out in this policy. Non-Municipal employee's access to the network is subject to the security policy. Consultants employed in a permanent capacity by the municipality are classified as municipal employees for the purposes of this policy. Part time contractors and consultants who may have access to municipal facilities, infrastructure, systems and information will be required to sign a confidentiality and security undertaking.

5. INFORMATION SECURITY DEFINITIONS

Information security encompasses the management processes, technology and assurance mechanisms that will allow departments 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.

6. HIGH LEVEL INFORMATION SECURITY PRINCIPLES

6.1 Protection

NDLAMBE's information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems, which process it (microcomputers, firewalls, voice mail systems, etc.), or the methods by which it moved (electronic mail, face-to-face conversation, etc.). Such protection includes restricting access to information based on a need-to-know basis. Municipal management must devote sufficient time and resources to ensure that information is properly protected.

6.2 Risk Management

Municipal managers are ultimately responsible to ensure that the information is protected in a manner that is acceptable to higher management. To achieve this objective, risks should be identified by conducting regular risk analysis and, to take corrective measures where applicable-

6.3 Information Management

Executive within NDLAMBE is also critically dependent on information and information systems. Management is expected to know the nature of information they use for decision making (accuracy,



relevance, completeness, confidentiality, criticality, etc-). The awareness of and fine tuning of such Information attributes is an important information management activity.

6.4 Co Operation

Information security requires the participation of and support from all information users. (employees, consultants, contractors, third parties and temporaries)

6.5 Organisation

Guidance, direction, and authority for information security activities is centralised for the entire organisation in the Office of the IT manager. The office is responsible for establishing and maintaining organisation wide information security policies, standards, guidelines, and procedures.

Compliance checking to ensure that organisational units are operating in a manner consistent with these requirements is the responsibility of the Internal/external Audit Department. Investigations of system intrusions and other information security incidents are the responsibility of the IT manager responsible for information and systems security.

6.6 Privacy

All messages sent over municipal computer and communications systems are the property of NDLAMBE. To properly maintain and manage this property, management reserves the right to examine all data stored in or transmitted by these systems. Since NDLAMBE's computer and communication systems are provided for business purposes, workers should have no expectation of privacy associated with the information they store in or send through these systems. In recognition of the privacy requirements as stated in the Constitution of South Africa, personal information will not be disclosed to any third party unless explicitly required through legal processes.

6.7 Third Party

As a condition of gaining access to NDLAMBE's computer network, every third party must secure its own connected systems in a manner consistent with the municipality's requirements. NDLAMBE reserves the right to audit the security measures in effect on these connected systems without warning. The municipality also reserves the right to immediately terminate network connections with all third-party systems not meeting such requirements

7. GENERALLY APPLICABLE POLICIES

The following policy statements constitute the core of the municipality's Information Security Policy for information and will be supported by information security directives and standards as needed from time to time.

7.1 Classification

Information must be categorised into levels of sensitivity and protected in accordance with Appropriate requirements as part of the risk management process. The sensitivity classification standard must be used throughout the municipality to ensure that the level of protection is commensurate with the controls required (security mechanisms) to protect the information against disclosure(confidentiality), modification (integrity) and / or destruction (availability and use).



7.2 Confidentiality

The confidentiality of all data, depending on classification and information security directives, will be protected before transmission over networks, and where indicated during the storage of such data. Unless authorised by management, information may not be made available or disclosed to unauthorised individuals, entities or processes. Measures should be implemented to protect information against unauthorised access, disclosure, copying, sniffing, eavesdropping and /or theft of information assets.

7.3 Availability

The continued availability and usability of services in accordance with business requirements must be ensured by implementing appropriate measures to prevent and recover from the loss of data due to acts of persons, system failures or disasters. All information assets should be protected against:

- Destruction, damage or contamination
- Denial of authorised / legitimate access
- Delay of use or access
- Natural disasters
- Computer virus infections

7.4 Integrity

The integrity of all data, depending on classification and information security directives, will be protected at all times before transmission over networks, and where indicated, also during the storage of such data. All information assets should be protected against threats to data integrity including unauthorised modification, destruction, and misrepresentation of data and / or computer virus infections.

7.5 Non-Repudiation

All access to the municipality's technology resource is subject to positive identification and authentication of the user before access is granted. Measures must be implemented to ensure the non-repudiation of all financial transactions in accordance with official legislation and regulations. Processes must be implemented to allow for the non-repudiation of origin regarding sensitive e-mail.

7.6 Accountability

Measures must be implemented to ensure that it is possible to determine who is responsible for an action, when and from where. The measures must be in accordance with the security requirements as determined by the departmental manager.

7.7 Access Control

All data and information will be protected and safeguarded against unauthorised access. Access to technology resources will only be granted in line with the user's specific responsibilities (need to-have principle).



7.8 Authentication

Measures must be implemented to uniquely identify or verify IT users, peripherals and / or programs and to assure individual accountability. The Authentication mechanisms must be in accordance with the classification of the information that requires protection and may for example take the form of passwords, tokens, or biometric identification devices. All users will access NDLAMBE's information systems through at least the use of a unique user identification number and secret password. As a first line of defence, users must select passwords that are not easily guessable nor should personal passwords be shared with any other user.

7.9 Reporting of Security Incidents

All known vulnerabilities- in addition to all suspected or known violations- must be reported in an expeditious and confidential manner to the Office of the IT manager. Unauthorised disclosure of the municipality's information must additionally be reported to the involved information owners. Reporting security violations, problems or vulnerabilities to any party outside the municipality without prior written approval of the Office of the IT manager is strictly prohibited. Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action.

7.10 Exceptions

Exclusions based on a valid business need could be motivated for and formally, in which case record would be kept of the exclusions to facilitate effective management / control processes.

8. MANAGEMENT POLICY

8.1 General Requirements

- Ownership - The Department responsible for IT is the owner of the policy. ‘
- Applications for remote access services will only be allowed to personnel and clients or contractors, based on a valid business need. All applications must be motivated and recommended in writing by the applicant's manager or the department / business unit requesting the access, and handed to the Manager responsible for IT. The manager will consider all applications for approval after consideration of the risk. Periodic access reviews will be conducted with the assistance of HR to ensure incumbents are still in the municipality's employ. All accesses must be reviewed at least annually by the applicant's manager and where applicable, terminated / suspended.
- As part of the application process and before access is allowed, the user(s) applicant should sign an agreement confirming that all policies and procedures (with specific reference to antivirus software on his / her computer) will be adhered to and that only licensed / legal software is installed on the computer.
- A central register must be maintained by the IT function or department responsible for IT of all users with dial in / remote accesses, also indicating the access authorities to facilitate auditable processes.
- In order to ensure compliance in terms of software, hardware and security requirements, the computer used for the remote access should be provided by the municipality. The use of private (home) computers may only be allowed if based on a valid business need and must be processed as a deviation from this policy. The manager/department responsible for IT shall maintain a central register of all the deviations.



- The remote client (computer used to access the municipality's network) must have anti-virus software and the correct level of security patches as prescribed by the IT function from time to time. A process must be formulated by the IT function to ensure the regular update of the software/patches.
- Under no circumstances may the access privileges be transferred to another user without following the official normal application procedure.
- No user may be provided with access privileges that exceed those than would otherwise be afforded if working in the office (least access /authorisation principle).
- To prevent an open session from being misused by unauthorised persons, all sessions must automatically be logged off after 30 minutes of inactivity.
- The users are responsible for both logical and physical security mechanisms to the computer that is used to obtain the remote access. Due to the risk of theft, users are advised to encrypt stored data for protection. The municipality's security requirements must be communicated to users. Comment: Logical access control refers to the measures taken to prevent an unauthorised person to get access to your computer whereas physical mechanisms relates to the physical measures taken (first and second perimeter of defence).
- Confidential information stored on remote computers must be protected against unauthorised access.
- Formal agreements with clients, partners, contractors or third parties is a requirement and must include the principle that required minimum standards compliance must be verifiable/auditable if remote access is provided.

8.2 Authentication Requirements

- Authentication servers must be configured to enforce the municipality's password standards. Strict physical and logical access control to the authentication servers and communication equipment must be enforced.
- As a minimum requirement, a unique user ID and difficult to guess password must be used for authentication.
- Users having power access privileges (e.g- to execute remote maintenance tasks and access to sensitive information and / or critical resources), may only be allowed access through the municipality's accepted authentication mechanisms. (Sensitive information is defined as information that if disclosed, will seriously and adversely affect the municipality, its business partners and / or clients and will constitute a serious compromise in the status of the municipality's operational security)
- A forced password change must be implemented on the first sign on session (to change the initial password) and thereafter every thirty (30) days. The IT function should implement a process to ensure the secure communication of the initial password.
- No double sessions with the same authentication information may be allowed.
- To confirm the origin of the connection, dial-back features must be implemented if token-based authentication is not utilised.
- Authentication information between the users and the authentication servers must be protected with encryption.
- Users no longer requiring the access (e.g. change in job description or transfer) must be immediately removed from the system. Line management must reconsider the access privileges of users who resign as soon as possible after formal notice of the resignation. Special attention should be given to audit logs to ensure that the accounts are no longer active.
- All changes to existing and new user accounts/profiles must follow a formal change management process.



- In support of the information security strategy to protect, detect and re-act, all available audit logs and alert facilities must be enabled with monitoring and review processes in place. The reports must be reviewed by the IT department and, where applicable, investigated / escalated to the manager responsible for IT.
- The municipality reserves the right to suspend / cancel any account(s) that acted in contradiction to this policy or any other procedural requirement as formulated from time to time.

8.3 Clear Screen and Clear Desk Policy

- At the end of each day, or when desks/offices are unoccupied, any 'Management in Confidence' or 'Classified' information must be locked away in either pedestals, filing cabinets or offices, as appropriate.
- All waste paper, which has any sensitive or important municipal information or data on, must be shredded or placed in the secure shredding boxes located in some areas. Under no circumstances should this type of waste paper be thrown away with normal rubbish in the bins under each desk.
- Whenever the user leaves their desk and the PC is switched on, it is essential that the user ALWAYS 'lock' their screen by pressing 'Ctrl Alt Delete' (for Windows Operating systems) and then enter to confirm that they wish to 'lock' their workstation. Remember that the user will need their password to sign on.
- Locking the screen not only prevents someone else from using the PC, which is logged on in the user's name, but it also prevents someone from reading sensitive information on the screen.

8.4 Passwords

Passwords must NEVER be disclosed to anyone. If the user suspects that the confidentiality of the password has been compromised, the user must change it immediately and inform the IT manager.

- Passwords must be changed every 30 days; the authentication server must be set to automatically expire passwords after 30 days.
- Passwords should be made up of characters using. Alpha (alphabetical letters), numeric (whole numbers), upper & lower case and symbols. They should have a minimum length of 8 characters.
- Never use any dictionary words, acronyms, birthdays, sequential numbers, family names, football teams; dates etc, as software tools can easily crack these (must not be easily guessable).
- Passwords should not be written down unless protected in some or other form (e.g. by using a sort of encryption and locking it away).
- The authentication server/system will maintain a list of up to 12 previous passwords used per user and each new password should contain at least 3 changes. The objective of this rule is to prevent users raising the same password over and over.

8.5 Access Control Policy

- Access to systems will only be granted where there is a clearly established business need, which is consistent with the roles and responsibilities of those granted access.
- Staff must not attempt to bypass the physical security mechanisms (turn stiles & trapdoors), or electronic (logical) security measures.
- The physical security steps taken are the first line of defence against unauthorised access to the municipality's information assets.



8.6 Virus Protection

- The IT department must always ensure that computers are equipped with an approved antivirus software package.
- Check removable media for viruses before they are opened and stored on the computer (the antivirus software should be set up to automatically perform the task).
- Train users not to open suspicious looking email. Always confirm the bona fides of the originator if uncertain about the contents.
- Users should check with the IT department before forwarding email about new viruses to colleagues. In many instances it is a false alarm with the intent to cause panic thereby flooding the network with unnecessary messages.
- When staff members are required to use their home personal computer for official municipal duties, the PC should have an antivirus program installed. The program should be updated regularly to ensure that provision is made for the latest viruses.

8.7 Account Policies

8.7.1 Password

- Enforce password - Only twelve (12) passwords will be remembered by the system. This will prevent the user from using the same password continuously- Should a user forget his/her password the system administrator must be contacted.
- Maximum password for expiry - Thirty (30) days, after which the user must enter and confirm a new password.
- Minimum password length - Eight (8) Characters that can be numerical or alpha numerical or a combination of both and include case changes and symbols.

8.7.2 Account Lockout Policy

- Account lockout duration - Permanent. To reset network administrator must be contacted.
- Account lockout threshold - Three (3) invalid login attempts will be permitted after which the user account will be locked. To reset the account the system administrator must be contacted. Users who do not log into systems with their user accounts (Munsoft, PayDay, e-mail, Domain and Route Master) for 30 days or longer will be locked out by I T Manager from accessing the system/s. The user must then apply in writing to his/her Director who must then approve of the reasons given before that account will be made active again.

8.7.3 General

- Enforce user logon restrictions - Enforced. Coupled to account logon hours.
- Maximum tolerance for computer clock synchronization - Five (5) minutes.
- All staff will be issued with one user access code/account per system (Munsoft, PayDay, e-mail, Domain, and Route Master) Current users with more than one user account will after amendment approved by Council be limited to one user code/account per system (Munsoft, PayDay, e-mail, Domain and Route Master)

8.8 Local Policies

8.8.1 Audit Policy

- Audit account logon events - Attempts will be logged on success and failure to logon to the network.
- Audit account management - Success and failure will be monitored daily.



- Audit directory service access - Success and failure will be monitored daily.
- Audit logon events - Success and failure will be monitored daily.
- Audit object access - Success and failure will be monitored daily.
- Audit policy change - Success and failure will be monitored daily.
- Audit privilege use - Success and failure will be monitored daily.
- Audit process tracking - Success and failure will be monitored daily.
- Audit system events - Success and failure will be monitored daily.

8.9 Security Options

- Automatically log off users when logon time expires - Logon hours will be between 07H00 and 18H00. After this time period users will be logged off by system. Any user that works after these hours must apply to the I.T. section for permission to change logon times.
- Do not display last user name in logon screen - Enabled.
- Prevent users from installing printer drivers - Enabled.
- Prevent users from installing software - Enabled.
- WWW Browser access - All browsers shall be configured to access the Internet via proxy servers or via a site proxy server, which is configured to access the Internet. No other form of access to sites on the Internet is permitted. This includes connections to alternative service providers by means of a dial-up modem, leased data line, private microwave link, radio modem or any other form of access method. Users shall be held liable for breaches of security, loss of data or the compromise of information caused by unsafe browsing practices.
- Firewall - A firewall will be installed to protect the municipalities internal networks and systems from external attack and penetration attempts. The creation of a demilitarised zone is preferred, but not mandated. This policy may be revised should the municipality experience a high incidence of penetration attempts- The firewall should be configured to provide at least the following: Network Address Translation (NAT). Proxy services. Port blocking and control. Packet sniffers. Intrusion Detection and virus attack protection. WWW management features. Logging of audit information. Custom rule formulation and configurations.

9. USER POLICY

- The access provided by the municipality is not to be used to access any material of a sexual, violent, destructive or potentially harmful nature. The system must be used in a moral and ethical manner.
- Due to system limitations, remote access connections may not be used for a period longer than 8 hours per day.
- Unless specifically specified, the municipality does not offer technical support for personal (home) computers.
- Password must be kept secret and may under no circumstances be disclosed or transferred to another user without following the official application process.
- Users are expected to report all breaches or suspected breaches of security to the manager of IT and their immediate manager.
- The account may not be used to conduct any illegal activities. It is the responsibility of management to ensure that the security policies are effectively communicated to users in order to establish accountability.



- The computer must be kept updated with the latest municipal accepted antivirus agent. The municipality employees can obtain a copy from the IT department/function.
- Users will be held accountable for actions committed under the specific user profile.
- Users may not leave their computers unattended with an open session. Users should either sign-off, activate a password screensaver, or lock the screen if the computer is unattended and still signed on.
- Users must respect copyright, trademark, licenses and related legislation. The service must be used in a manner that does not interfere or disrupt other network users, services and / or equipment.


10. LEGAL AND REGULATORY REQUIREMENTS

Although the personal use of the municipality's information systems is allowed within limits, abuse of these systems and the use of obscene, racist or otherwise offensive statements are strictly prohibited.

11. DISCIPLINARY CODE OF PRACTISE

Refusal to adhere to this policy will be considered as misconduct and depending on the circumstances and seriousness of the offence, disciplinary action may take, inter alia, one of the following forms:

- Disciplinary Counselling
- Verbal Warning
- Written Warning
- Termination of Service; or
- Summary Dismissal

Action	1st Occurrence	2nd Occurrence	3rd Occurrence
Changing any configuration settings to bypass security or any other control mechanism thereby exposing the valuable municipal assets	Final written warning 	Dismissal	
Allow another user on municipal network with your account details and password	Written warning	Final written warning	Dismissal
Using the account of another user to obtain unauthorized access to data, files or network services	Written warning	Final written warning	Dismissal
Any attempt to test or bypass security mechanisms and or processes	Final written warning	Dismissal	
Abusing specific resources or services e.g. email or internet	Written warning	Suspension of remote access and final written warning	Dismissal
Loss of municipality's assets e.g. laptops due to negligence (theft out of vehicle left unattended with valuable municipal asset)	Written warning	Suspension of remote access privilege, final written warning and replacement of asset.	Dismissal
Infecting the municipality's network with viruses by neglecting to install and update / removing the prescribed anti-virus agent on the remote computer.	Final written warning	Dismissal	
Failure to report unauthorized policy / standard deviations or security incidents.	Written warning	Final written warning	Dismissal
Loading illegal software, thereby infecting the municipal network with viruses or trojan horses.	Final written warning / Dismissal	Dismissal	
Willfully downloading and/or opening virus infected files	Final written warning	Dismissal	
Disabling, uninstalling or changing the original configuration of the municipality's anti-virus product unless specifically authorized to do so	Written warning	Final written warning	Dismissal
The configuration and use of unauthenticated shares	Written warning	Final written warning	Dismissal



12 IMPLEMENTATION PLANS

Subject Channel /: Actions	
Top-down communication	Communication of policy existence by members of the Information Technology Steering Committee to respective business and IT areas they represent. Communication to management of members not having representation on the Steering Committee
Awareness	Publication on Intranet and Bulletin Board system (if available). Prepare electronic presentation with security and operating requirements for users. Request new and existing users to acknowledge receipt of policy and to sign confirmation of compliance. Prepare broadcast message for existing users indicating the location of the policy.
Management Issues	Determine current compliance to policy and define gaps. Define plan of action to align with policy List residual risks and management plans. Review and update dial-up connection processes. Continuous monitoring of compliance. Regular review and dissemination of policy.

13 EFFECTIVE DATE

This policy comes into effect on _____



14 COMPLIANCE AGREEMENT

AGREEMENT TO COMPLY WITH INFORMATION SECURITY POLICIES

User's Clearly Printed Name:

User Signature

E-mail@ndlambe.gov.za

Employee No:

Department:

Job Title:

User's Telephone Number:

I, the user, agree to take all reasonable precautions to assure that the municipality's internal information, or information which has been entrusted to the municipalities by third parties (such as customers), will not be disclosed to unauthorised persons. I understand that I am not authorised to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Municipal Manager who is the designated information owner. I agree to return to the municipality all information to which I have had access as a result of my position with the municipality on termination of my employment or contract with the municipality-. I have access to copies of the municipality's Information Security Policies, I have read and understand the contents of the Policy(s), and I understand how it impacts my position in the municipality. As a condition of continued employment at the municipality, I agree to abide by these information security policies. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from the municipality, and perhaps criminal and/or civil penalties. I agree to choose a difficult-to-guess password as described in the municipality's information Security Password Standards document as discussed in this policy. I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognisable way. I will ensure that only legal and licensed software is installed on the computer and accepts that the municipality cannot be held liable for any violations due to my actions. I also agree to promptly report all violations or suspected violations of information security policies to the manager of IT and my direct manager. I agree that the terms and conditions of this Compliance Agreement are both reasonable and necessary for the protection of the municipality's internal information, or information which has been entrusted to the municipality by third parties.

User.....

User's Manager:

Signature:

Signature:

Date:

Date:

Document Control Sheet

NDLAMBE MUNICIPALITY

IT DATA and SYSTEMS SECURITY POLICY



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

Department I.T Document Number 2020-04 Revision Issue Date 2020/??/??