ICT NETWORK SECURITY POLICY
2024/25

Table of Contents

S.S.K

LIST OF TABLES

APPROVAL AND REVISION HISTORY

APPROVAL SIGNATURES RECORD			
APPROVALS	**CHAIRPERSON NAME**	**SIGNATURE**	**DATE**

REVISION NUMBER	PAGE NUMBER/S	CHANGES EFFECTED	DATE OF CHANGE
0.1	1-19	First draft created	24-10-2022
	1-19	Policy review	14-06-2024

S.S.K

GLOSSARY OF TERMS AND ABBREVIATIONS

Table 1: Terms and Abbreviations

Term/Abbreviation	Definition
Access Control	A system to restrict the activities of users and processes based on the need to know.
Communication Carrier	The infrastructure provided by a service provider to interconnect communication devices.
Computer Network	A range of computers connected by means of communication carriers.
Control Mechanisms	Refers to ICT controls such as policies, procedures and activities put in place by an organisation to ensure the confidentiality, integrity and availability of its ICT systems and data.
Data Traffic	Information in electronic format, which is communicated over a communications carrier.
Encryption	A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.
Firewall	A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have passed some security check, such as providing a password.
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.
IP	Internet Protocol
IP Address	An essential networking element which permits traffic to be routed to a specific host
LAN	A local area network(LAN) is a collection of devices connected together in one physical location
Network Device	Any information and communication technology device used to form the infrastructure required for communication services (servers, routers, switches, bridges, firewalls, encryption devices).

S.G.K

Term/Abbreviation	Definition
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 Sniffing	The use of hardware and/or software mechanisms to analyse / monitor electronic communications (traffic) over a network.
Non IP Network	Emphasises that the technology is not dependent on IP packet formats or protocols.
Operational Environment	The environment responsible for the implementation and maintenance of the day to-day security activities.
Patches	A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes, and improving the usability or performance.
Sensitive Information	Any information that, if disclosed without appropriate authorisation, will compromise the Municipality's security or business initiatives.
Sniffing	The use of hardware and/or software mechanisms to analyse / monitor electronic communications (traffic) over a network.
Spyware	A class of programs designed to steal personal information.

S.9K

1. INTRODUCTION

1.1. 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 making it difficult to draw boundaries around the Municipality and to apply controls for the protection of the internal assets.

2. PURPOSE

2.1. The purpose of this policy is to provide a solid foundation for the development, implementation and maintenance of secure practice within the Mandeni Local Municipality (MLM also hereinafter referred to as "the Municipality") networking environment.

3. SCOPE

3.1. This policy applies to all who access Municipality computer networks. Throughout this policy, the word "user" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems administered by Mandeni Local Municipality or its partners.

4. LEGISLATIVE FRAMEWORK

4.1. The policy was developed with the legislative environment in mind. The following legislation, amongst others, were considered in the drafting of this policy:

- 4.1.1. SA Minimum Information Security Standards
- 4.1.2. ISO/IEC 27001:2005 Specification for an Information Security Management system
- 4.1.3. ISO 31000 Risk management - Principles and guidelines
- 4.1.4. Professional Codes of Conduct and Guidance
- 4.1.5. Protection of Personal Information Act, Act No. 4 of 2013

S.B.K

5. GENERAL POLICY REQUIREMENT

5.1. 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.

6. AUTHENTICATION

6.1. Windows active directory shall be used to manage all user authentications to the domain; every user shall be forced to join the domain and shall only work on the network if they are authenticated. Any user who fails to follow this protocol and or bypasses the system security shall be taken to a disciplinary enquiry.

6.2. Passwords must be implemented in accordance with the Municipality's password standards.

7. PASSWORD SETTING

7.1. Formal set-up standards must be agreed on 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.

7.2. Administrator account password should at least be nine characters long and that it includes at least one punctuation mark or non-printing ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronised across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

7.3. Users must change passwords after every 30 days, if a user has forgotten his/her password or if the password expires then the user must request the ICT division to change his/her password by completing the relevant forms and submitting them to the ICT division.

8. PROTECTING PASSWORDS

S.G.K

8.1. Users are strictly prohibited from sharing passwords and it is their duty to ensure that the passwords are unique and are protected from other users. Passwords are not to be written or said out loud.

9. SET STRONGER PASSWORD POLICIES

9.1. The minimum password length to be at least six (6) characters.
9.2. The minimum password history appropriate to network shall be seven (7) days).
9.3. The maximum password age appropriate to network (typically no more than 30 days).
9.4. Should not set a password history maintenance (using the "Remember passwords" option).
9.5. At least three (3) of the following four (4) requirements must be met:
  9.5.1. Must contain an upper case letter (A-Z)
  9.5.2. Must contain a lower case letter (a-z)
  9.5.3. Must contain a numeric character (0-9)
  9.5.4. Must contain a special character (! #@…)

10. LOGICAL ACCESS CONTROL

10.1. 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. External access to network devices must be restricted to the minimum and where applicable, strict control mechanisms must be implemented.
10.2. Individual user IDs should be used.
10.3. User IDs will not be shared unless senior management authorisation is approved.
10.4. Access granted to users should be based on what the user needs to do their job and no more.
10.5. Lock outs – screen savers should be implemented to automatically lock screens.
10.6. Limit duplicate log-ins by the same user wherever feasible.
10.7. Consider setting timed limits for access.

11. PRIVACY / CONFIDENTIALITY

S.S.K

11.1. Users are responsible for the integrity of all data, and must protect MLM data from unauthorised access. At any time and without prior notice, the Municipality management reserves the right to examine email, personal files and other information stored on its equipment.

12. ENCRYPTION

12.1. A certificate authority server shall be installed for encryption and decryption of data over the Network; encryption will be used when accessing the network remotely via VPN or Web Access. All data classified as confidential, secret and Top secrete shall be password protected and encrypted if sent over electronic mail.

13. VIRUSES, MALICIOUS SOFTWARE

13.1. Formal processes must be implemented to ensure that all applicable security patches are kept updated.
13.2. MLM shall utilize ESET Complete Endpoint antivirus and ESET for Servers with file and mail filtering for maximum protection against malware, adware, viruses… etc.
13.3. Users are prohibited from disabling, cancelling or deleting antivirus software or any other software installed by the ICT division on Municipal ICT equipment and may not change any configuration setting on their computers.
13.4. ICT will notify users in advance via email or system notification if there is an upgrade or replacement of the antivirus software or updates to the firmware and software.
13.5. Only the ICT division is allowed to test software on Municipal ICT infrastructure.
13.6. ICT may further Implement anti-spyware to protect private information.
13.7. Regularly check for vendor security updates and apply them.
13.8. Enable the built-in firewall that is included in the major operating systems and/or install a firewall application.

14. INTEGRITY

14.1. 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.

S.S.K

15. AVAILABILITY

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

16. MOBILE COMPUTING AND WORKING AT HOME

16.1. Any user requiring remote access into the network must be authorised by the Municipal Manager. Remote access shall be location independent for wireless connection however such access will be restricted via password authentication or VPN client authentication.

16.2. 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.

16.3. 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.

17. AUDIT LOGGING / ACCOUNTABILITY

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

18. INTERNET USE

18.1. Users must adhere to the following precautions when surfing the Internet:

18.1.1. Do not spend more than one hour a day on the internet.

18.1.2. Do not enable automatic password saving.

18.1.3. Avoid installing software from the Internet without the ICT division's authority.

18.1.4. Do not enable pop-ups, active x and downloads of any other software.

S.S.K

18.1.5. ICT will request security reports from time to time on Internet usage and users will be required to submit these reports. False security reporting will result in disciplinary action.

19. EMAIL USE

19.1. It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
19.2. Do not forward a message without acquiring permission from the sender first.
19.3. Do not send unsolicited email messages.
19.4. Do not forge or attempt to forge email message.
19.5. Do not send email message using another person's account.
19.6. Do not copy a message or attachment belonging to another user without permission of the originator.
19.7. Do not disguise or attempt to disguise your identity when sending email.
19.8. All email accounts maintained on Municipal email systems are property of Municipality. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.
19.9. Scan all email attachments before opening them.

20. NETWORK MANAGEMENT

20.1. Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

20.2. Users of Municipality's information resources must not access computer software, computer data or information, or networks without proper authorisation, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the Municipality.

20.3. 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 this information. Documentation must be in accordance with the sensitivity / security classification.

S.S.K

20.4. Any default discovered in system accounting or system security must be reported to the appropriate system administrator so that steps can be taken to investigate and resolve the problem.

20.5. Non IP network connections must be secured by definition characteristics and / or specific configurations to restrict access capabilities and to meet the security requirements.

20.6. 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.

20.7. 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.

21. TRAFFIC MANAGEMENT

21.1. Network devices must be configured to prevent unauthorised access.
21.2. The configuration(s) must be reviewed at least annually or after significant changes and health checked at least once every quarter.
21.3. Unauthorised changes must be handled as a breach of security.
21.4. 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 ICT Manager.
21.5. Measures must be implemented to ensure the network filtering devices cannot be bypassed and can only be accessed from specified IP addresses via authorised secure channels.
21.6. Broadcast of information about the network must be restricted to the absolute minimum.
21.7. Traffic flowing over the network must be afforded the same protection / security characteristics as when stored in accordance with the classifications of the information.

S.B.K

22. NETWORK OPERATIONS

22.1. All unusual entries / activities must be investigated and reported to appropriate line management for corrective action.

22.2. Pre-authorised intrusion detection mechanisms should be employed as protection against possible attacks.

22.3. Effective incident response, business continuity and disaster recovery planning processes must be implemented.

22.4. Network changes must be documented, formally accepted by the network owner and follow an accepted Change Control Policy and standard.

22.5. 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.

22.6. To reduce the risk of data in transit being intercepted, special care must be taken to protect network cables from tampering or disruption.

22.7. Back-up versions of essential network information and software 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.

22.8. Remote maintenance must be controlled by restricting access rights and logging all activity. Diagnostic ports on network equipment must be protected by access controls.

22.9. Access to network devices that are primarily used for security services must be approved by the ICT Manager.

22.10. Access to any other network devices must be regulated via a formal process to request and authorise access.

22.11. 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.

S.G.K

22.12. Internal or external remote maintenance sessions to devices that form the security barrier may not be allowed unless protected / controlled through a secure channel.

22.13. No modems may be connected to the network without the prior approval of the applicant's line and ICT Manager. A register of all approved modems must be maintained.

23. RISK MANAGEMENT

23.1. A formal risk analysis must be carried out at least annually for networks that support critical business applications.

23.2. 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.

23.3. 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 the management.

23.4. 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.

23.5. 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.

23.6. Create regular backups of your data and files.

24. FRONT END PHERIPHERAL USAGE

24.1. The ICT division shall be responsible for designing the specifications for any front end peripheral and shall also configure, maintain and support the peripheral. The network administrator shall ensure that all peripherals are secured and users shall not temper to remove, install or open the peripherals.

S.S.K

25. BACKUP AND RESTORE

25.1. Backup of all data and applications shall be done daily, off which they will be done remotely to Umhlali site. This should also include the replication which must also be done remotely. The full backup will be run on daily basis.

25.2. Backup testing shall be carried out to ensure that a backup has been successful and a restoration option is available.

25.3. These disaster recovery practices should also be scheduled and be done.

25.4. Any changes that are introduced to backup configuration should also result in an additional backup and restore tests and the backup restoration plan should be updated accordingly.

26. SERVICES

26.1. In order to add a new server to the network, ICT should configure the server and then complete and forward a Server Request Form to the ICT Manager for approval.

26.2. All servers must be configured with static IP addresses according to the Municipality's IP addressing guidelines.

26.3. Minimum configurations on server shall be provided by the ICT division and ICT shall ensure that these configurations are updated quarterly.

27. POLICY ENFORCEMENT

27.1. Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to Municipality Information Systems. Additional administrative sanctions may apply; up to and including termination of employment or contract with the Municipality. Criminal and equitable remedies may also apply.

28. PRINCIPLES

S.G.K

28.1. Access to network services is to be restricted to verified users, devices and applications;

28.2. Where an automated process is used to connect remote systems, a suitably secure authentication mechanism which meets the information security standards must be used in the process;

28.3. Cross boundary access between internal and external networks is to be secure and must use an information security approved authentication method at the entry points;

28.4. Remote access to Municipality systems is to be managed as outlined in Municipality Access Management Policy.

28.5. Network connections with external environments must prevent unauthorised access.

29. RESPONSIBILITIES

29.1. System administrators are responsible for:

29.1.1. Promoting information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.

29.1.2. Taking precautions against theft of or damage to the system components.

29.1.3. Faithfully executing all hardware and software licensing agreements applicable to the system.

29.1.4. Temporarily suspending access privileges if it is necessary or appropriate to maintain the integrity of the computer system or network.

29.2. ICT Manager is responsible for:

29.2.1. Network Strategy Formulation;

S.S.K

29.2.2. Implementation of Policy;
29.2.3. Policy Update / Revision;
29.2.4. Compliance Monitoring;
29.2.5. Reports Monitoring;
29.2.6. Management of Information;
29.2.7. Reporting of Security Incidents;
29.2.8. Formulation of Operational Processes;
29.2.9. Formulation of Technical Network Standards;
29.2.10. Risk Analysis;
29.2.11. Centralised Access Control;
29.2.12. Network Inventory;
29.2.13. Network Security Device Management;
29.2.14. Approval of Third-Party Connections;
29.2.15. Network Contingency Planning (including disaster recovery); and
29.2.16. Compliance reviews from a management perspective.

29.3. Internal Audit is responsible for:
29.3.1. Annual revision of the policy.

30. POLICY REVIEW

30.1. This policy shall be reviewed annually to accommodate the variances. Any amendments to this policy must be submitted to the ICT Steering Committee by the head of departments. The ICT division will affect the necessary changes and the policy will be approved in terms of the Municipality's policy approval process.

31. NON-COMPLIANCE

31.1. Unless specifically and formally approved by the ICT Manager, any deviation from this policy is strictly prohibited.

31.2. 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.

S.S.K

32. OTHER RELATED DOCUMENTS

32.1. Business Continuity Plan
32.2. ICT Disaster Recovery Plan
32.3. Disaster Recovery Policy
32.4. ICT Governance Framework
32.5. Backup procedures
32.6. Network Diagrams

PREPARED BY: P.E NTANZI

DATE OF ADOPTION BY COUNCIL: 10 JULY 2024

COUNCIL RESOLUTION NO: C01

MUNICIPAL MANAGER

S.G KHUZWAYO

11/07/2024

DATE