CAPE WINELANDS DISTRICT
MUNICIPALITY • MUNISIPALITEIT • UMASIPALA

NETWORK SECURITY POLICY

Revision History

Item No.	Author	Date	Revision
C.14.1	ICT	25 July 2013	Policy Adopted by Council
C.14.1	ICT	24 April 2014	Policy reviewed and Amended
C.15.1	ICT	19 September 2016	Revision by ICT steering committee

This document has been approved by

Item No.	Author	Date	Approval
C.15.1	ICT	25 April 2017	Council

TABLE OF CONTENTS

1. INTRODUCTION

The availability and integrity of the Cape Winelands District Municipality (CWDM) Information and Communication Technology (ICT) infrastructure (network, systems and workstations) can be severely compromised if not adequately protected from the continually emerging threats of today. Due to the rapid changing nature of technology, systems hardware and software configuration settings are inadequate to provide the required level of protection, necessitating additional protection mechanisms to reduce the risk or exposure that exists.

2. LEGISLATIVE FRAMEWORK

2.1 The following legislation, amongst others, were considered in the drafting of this policy:

2.1.1 Copyright Act, 1978 (Act No. 98 of 1978);

2.1.2 Electronic Communications and Transactions Act, Act No. 25 of 2002;

2.1.3 Minimum Information Security Standards, as approved by Cabinet in 1996;

2.1.4 Municipal Finance Management Act, 2003 (Act No. 56 of 2003);

2.1.5 Municipal Structures Act, 1998 (Act No. 117 of 1998);

2.1.6 Municipal Systems Act, 2000 (Act No. 32, of 2000);

2.1.7 National Archives and Record Service of South Africa Act, Act No. 43 of 1996;

2.1.8 Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

2.1.9 Protection of Personal Information Act, 2013 (Act No. 4 of 2013);

2.1.10 Regulation of Interception of Communications Act, 2002 (Act No. 70 of 2002); and

2.1.11 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

2.2 The following internationally recognized ICT standards were leveraged in the development of this policy:

2.2.1 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;

2.2.2 Control Objectives for Information Technology (COBIT) 5, 2012;

2.2.3 ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls;

2.2.4 King Code of Governance Principles, 2009; and

2.2.5 Centre for Internet Security – Security Benchmarks, 2014.

3. POLICY PURPOSE, OBJECTIVE AND APPLICATION

3.1 The purpose of this policy is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of the Cape Winelands District Municipality's (CWDM) information handled by computer networks.

3.2 The objective of this policy is to protect the CWDM's information assets by defining what the minimum/baseline security requirements are that will provide the additional protection to preserve the confidentiality, integrity and availability of these assets.

3.3 It must be noted that, as technology advances, the requirements for protection could change resulting in additional deployment of hardware and software security solutions.

3.3 This document supports a layered defense strategy to facilitate the implementation of the minimum security requirements of effective and efficient security solutions.

3.5 This policy applies to all who access the Cape Winelands District Municipality's 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 owned by or administered by the Cape Winelands District Municipality.

4. ABBREVIATIONS

Abbreviation	**Definition**
ACL	Access Control List
AVS	Anti-Virus Software
CWDM	Cape Winelands District Municipality
ICT	Information & Communication Technology
NAC	Network Access Control

SSL	Secure Socket Layer
VPN	Virtual Private Network
WAP	Wireless Access Point

5. DEFINITIONS

Terminology	**Definition**
Administrator	An individual or group who is responsible for the day-to-day maintenance and operation of the information systems. An "end-user" is everyone else.
Anti-Virus Software	A computer software used to prevent, detect and remove malicious software.
Cape Winelands District Municipality's information	i. Any information within its purview, including information which the District Municipality may not own but which is governed by laws and regulations to which the District Municipality is held accountable. It includes data in any form, that is owned and used by the District Municipality to conduct its business, and which is captured, stored, maintained, and accessed in the District Municipality's systems (e.g. all client record data, all personnel data, all financial data, all administrative data, and all other data that pertains to, or supports the administration of the District Municipality). ii. All information stored in the District Municipality computers, or travelling over the computer networks that has not been specifically identified as the property of other parties, will be treated as though it is a District Municipality asset. It is policy to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is policy to protect information belonging to other parties that have been entrusted to the Municipality in confidence.
Confidential information	This includes: i. Information that has strategic value to the Cape Winelands District Municipality (CWDM) and which if disclosed, could harm the CWDM. ii. Information which has been defined as confidential. iii. Information which does not have either a public or a confidential designation must be treated as though it were confidential until its owner designates a fitting classification. In addition information belonging to third parties that has been entrusted to the Cape Winelands District Municipality must be treated as though it were confidential unless a contract or some other written agreement specifies otherwise. iv. Information provided by third parties and designated by them as confidential. v. Information provided to third parties and designated as confidential.
Cryptography	A method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Decision maker	The person(s) responsible for making decisions regarding access to, and use of, information systems and assets. In most cases, this is firstly the user's Department Head and secondly, the ICT Department.
Encryption	The process of encoding messages or information in such a way that only authorized parties can access it.
Firewall	A network security system designed to prevent unauthorised access to or from a private network. It can be implemented with both hardware and software.
Patch Management	A strategy for managing updates or upgrades for software applications and technologies
Secure Socket Layer	The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and structural.
Support	Generically, this refers to any organisation, body or person supporting the information systems.
User	This policy applies to all persons who access the information systems, regardless of whether such individuals are employees of Cape Winelands District Municipality. This includes all employees, contractors; outsource partners, consultants, temporary employees, and other workers, including those workers affiliated with third parties who access the information systems. Throughout this policy, the term "user" will be used to collectively refer to all such individuals.
Virtual Private Network (VPN)	A technology that creates an encrypted connection over a less secure network. The benefit of using a secure VPN is it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it.
Wireless Access Point	In computer networking, it is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.
Workstation	Any device that is used to gain access to information systems or assets. This includes but is not limited to: i. Personal Computer. ii. Laptop, tablet or notebook. iii. Terminal. iv. Network and non-network computer.

6. TARGET AUDIENCE

All CWDM Information and Communication Technology employed staff, including temporary employees, contractors, advisors, consultants, outsource partners and third parties, including those of subsidiary entities within the Cape Winelands group.

7. ENVIRONMENT

This policy applies to all systems, including but not limited to network, applications and support, within the Cape Winelands environment whether connected or standalone to the CWDM network and used for business or support purposes.

8. VIOLATIONS

This policy is an extension to the Cape Winelands District Municipality User Security Policy. Any violation of this Policy may result in disciplinary action, which could lead to dismissal, revoking of access privileges, or termination of agreement or contract. The CWDM's disciplinary procedure will be initiated by the line manager, or failing this, will be initiated by the designated process owner(s) of the process(es) affected by this policy.

9. GENERAL

9.1 The documented security requirements as well as solutions, tools and utilities must be implemented within the Cape Winelands District Municipality's network perimeter to ensure adequate protection against known and unknown threats.

9.2 Any project, or enhancement to an existing system that increases the risk, exposure or vulnerabilities to the systems environment, must provide the additional security protection mechanisms to mitigate the risk, exposure or vulnerability.

9.3 Additional support processes, procedures and standards must also be defined and implemented to aid and sustain the effective management of these security solutions.

9.4 All ICT personnel are required to sign Confidentiality agreements in order to safeguard information on the Cape Winelands District Municipality Network and Systems.

9.5 Whilst this policy contains explicit guidelines for network security, the main issue is finding ways and means to use all of the Cape Winelands District Municipality's resources to promote its business goals. This means the use of the network exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, it is expected that authorized users conduct themselves in a business-like, honest and accountable manner when using the municipal network.

9.6 All information carried over the Cape Winelands District Municipality's computer networks that has not been specifically identified as the property of other parties will be treated as though it is a Cape Winelands District Municipality asset.

It is the policy of the District Municipality to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is the policy of the Cape Winelands District Municipality to protect information belonging to third parties that have been

entrusted to the District Municipality in a manner consistent with its sensitivity and in accordance with all applicable agreements.

10. NETWORK PROTECTION REQUIREMENTS

The network, in this case the local area network (LAN), is the backbone that connects all CWDM servers together providing access to systems to all or selective users within the CWDM. The LAN is extended beyond head office to connect or provide access to the CWDM region, and business partners through the wide area network (WAN). In order to provide connectivity to the outside world the LAN is connected to the internet, providing access to remote users.

10.1. Firewall

The firewall is a product that allows for a definitive set of rules governing the transmission or receipt of data between systems within the CWDM network and untrusted external parties.

10.1.1 At least one (1) firewall is required at the CWDM's main entry point to the Internet.

10.1.2 A firewall is required at every entry and exit point into the LAN or WAN where the connecting entity in turn is connected to another untrusted network and/or the internet.

10.1.3 A router with an effectively managed Access Control List (ACL) will be allowed concerning exceptional cases for external semi-trusted entities. These exceptions must be approved by the Manager: Information Technology.

10.1.4 All external connections from the CWDM network to untrusted parties must be done through the firewall10.1.5 Connectivity to business partners, who in turn have their own or independent access to the internet, will only be allowed where there is a reputable and robust firewall in place and is active.

10.1.5 Where possible, point to point access through the firewall must be implemented.

10.1.6 Quarterly reviews of the firewall infrastructure must be undertaken:

(a) Firewall rules must be reviewed for accuracy and effectiveness.

(b) A penetration test must be conducted to detect unnecessary open ports and illegal access points.

(c) A vulnerability scan must be performed to ensure that security standards are properly applied.

10.1.8 Firewall infrastructure and rules are administered by an outsourced partner:

(a) A firewall support agreement and service level agreement must be in place stipulating support requirements.

(b) Configuration standards must be applied according the approved secure configuration standard documents.

(c) The 3rd Party Firewall Change Request Procedure must be followed and final approval obtained from the Manager: Information Technology before any changes to the firewall rules are applied.

10.2. Cryptography

A data classification exercise must be conducted to determine what stored and transmitted data is sensitive to ensure that the acceptable level of security protection is assigned and implemented.

10.2.1. Field, Disk or Folder Encryption

Administrators must ensure that any stored data on servers or desktops that is of a sensitive nature must be encrypted. The following is the minimum requirements for CWDM to protect sensitive stored data of personnel (HR data), partners, clients and their customers:

(a) Password fields must be encrypted or hashed to ensure that hackers are not able to see or launch a dictionary attack to gain illegal access to the network or systems.

(b) Folders and files containing confidential data or voice recordings must be encrypted with reliable industry standard software.

10.2.2. Virtual Private Network (VPN)

VPN's provide secure transmission tunnel between two (2) points via the internet. The following is the minimum requirements for the Cape Winelands District Municipality to communicate and transmit securely with external parties through a permanent or temporary link:

(a) A firewall access form must be completed and the documented firewall approval procedure must be followed as the access is defined through the firewall.

(b) VPN encryption is reserved for highly critical or confidential business transmissions only as it requires a seat license for every client module per machine. The seat license must be paid by the user's cost centre.

(c) The VPN connection must be restricted to the access required only (point to point) and network access will only be allowed for the Municipal Manager and Heads of Department, and other employees subject to the prior approval of the applicable Head of Department.

10.2.3. Secure Data Transmissions (Network and Internet)

All sensitive data transmitted via the CWDM network and external internet must be encrypted with an industry standard encryption methodology to protect its confidentiality and integrity.

(a) Secure Sockets Layer (SSL) protocol (certificates) is a secure transmission method that must be used to protect web traffic.

(b) VPN's (IPSec protocol) can be used, as described above to create a secure tunnel for secure communications between two points.

10.3. Remote Login

Remote logins can place the network and systems environment under serious threat from unauthorised access. Multi factor user authentication is therefore of utmost importance.

10.3.1. External Remote access

Any external remote access must cater for 2-factor authentication.

10.3.2. Internal Remote access

(a) Remote access to servers for support must cater for 2-factor authentication.

(b) Any internal remote access to a user desktop/laptop must cater for user challenge and response. The user must confirm or give permission for administrative support access, unless approved by the Manager: Information Technology.

10.4. Wireless Network Access

Wireless access relieves the need for physical network cabling and connectivity. Wireless Access Points (WAP's) may be available to users for ease of connectivity and mobility. Care should be taken to secure access points and that user access is managed and controlled.

10.4.1 WAP's must be hardened and secured.

10.4.2 WAP's must be configured with the necessary authentication methods/standards to prevent illegal access to the network.

10.4.3 Quarterly vulnerability scans (e.g. Netstumbler walkabouts) must be conducted to:

(a) Detect and confirm the available and authorised WAP's.

(b) Detect access vulnerabilities on the WAP's.

(c) Ensure that configuration standards are applied.

10.5. Content Filtering

Content filtering is of paramount importance to regulate and inspect e-mail attachments as well as internet downloads for abnormal or destructive content. Malware can be introduced in many other ways internally on the CWDM network. Appropriate measures must be put in place to detect and remove these.

10.5.1. Proxy Server & Uniform Resource Locator (URL) Filtering

The proxy server provides a primitive method of blocking undesired websites. A comprehensive URL filtering tool, that includes a managed update service, must be implemented to effectively block access and downloads from undesirable websites.

10.5.2. E-mail & Internet Filtering

Viruses pose a serious threat nowadays and having an e-mail & internet filtering tool in place is vital. Current e-mail & internet filtering tools are rules based and must be implemented with managed rules update service.

10.5.3. Anti-Virus Software(AVS)

(a) AVS must be integrated with the resident e-mail & internet filtering tool to facilitate an effective virus blocking combination.

(b) Anti-virus software must be loaded and active on servers, desktops and mobile devices to detect, block and remove viruses, trojans, adware, malware and key-loggers.

(c) An effective and automated AVS update procedure must be in place to ensure that virus signatures are regularly updated.

(d) The update process must be monitored and checked regularly for database update as well as target infrastructure update failures.

(e) Users must not intercept or interrupt the scanning processes as this could expose the user computer to security threats and vulnerabilities.

(f) Users are responsible for damage occurring because of viruses on computer systems due to their negligence on scanning processes. When a once a virus is detected, the user must immediately call the Division: Information and Communication Technology for remedial action/s.

10.6. Vulnerability Management

It is important that regular network and server (including mainframe and application servers) vulnerability assessments are conducted to detect any existing configuration errors or system vulnerabilities.

10.6.1 At least four (4) independent external penetration tests must be completed per annum.

10.6.2 At least four (4) independent vulnerability assessments must be completed per annum.

10.6.3 A vulnerability management tool must be deployed to identify existing vulnerabilities at least on a quarterly basis per network segment.

10.6.4 Any vulnerability detected / reported must be immediately addressed/fixed.

10.7. Patch Management

Operating systems and system software have inherent programming errors that hackers and malicious software exploit to gain illegal access to networks and business systems.

10.7.1 Patch updates must be performed immediately for high risk vulnerabilities as emergencies, otherwise to be scheduled for a weekly automated update.

10.7.2 An automated patch management tool must be deployed to patch software vulnerabilities, as well as facilitate accuracy and speed.

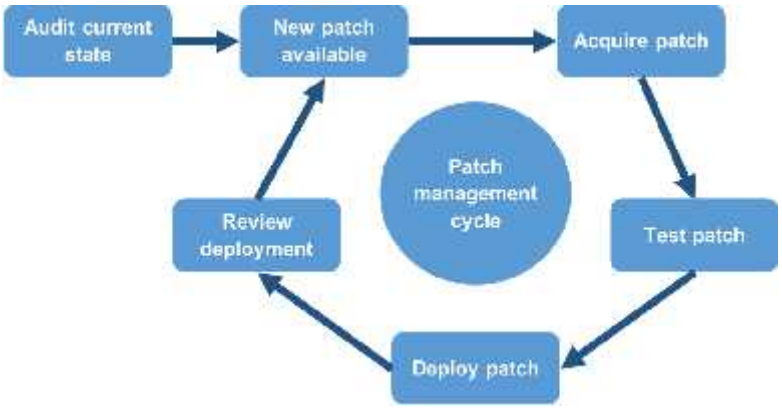
10.7.3 A patch management update procedure must be followed to ensure that current vulnerabilities are identified, remedied (patched) and appropriately managed.

10.7.4 Reports of unpatched vulnerabilities must be used to manually remediate vulnerabilities.

10.7.5 Servers and desktops not supported by the automated tool, must be physically visited and the patch updates loaded manually.

10.7.6 Automatic rebooting of patched devices will only be allowed for desktops and laptops on the network. Servers must be manually rebooted.

10.7.7 The below diagram depicts the formal patch management process to be followed:



10.8. Network Point Security

10.8.1 Specific network routers and switches have the capability to control access through Access Control Lists (ACL's) or Network Access Controls (NAC's).

10.8.2 Where possible these ACL's/NAC's must be used to serve as a first line defence against intruders.

10.9. Server and Workstation Lockdown

10.9.1 Servers, desktops and laptops must be locked down to prevent theft, illegal access or hacking attempts.

10.9.2 Administrators / technicians must ensure that the appropriate lockdown and configuration standards are implemented to prevent or minimise unnecessary security incidents.

10.10 Laptops, Mobile and Smart Devices

Employees in the possession of portable, laptop, notebook, handheld tablet and other transportable computers containing confidential information must not leave these computers unattended at any time, unless the information is stored in encrypted form.

11. SECURE AREAS

Certain areas where data processing, storage and communications are facilitated must be secured to prevent illegal entry, theft or systems access. The appropriate security standards must be implemented to ensure secure areas.

11.1. Secure Processing (Server & Network Rooms)

11.1.1 Server and network (including switch) rooms house access control and critical business infrastructure and must be protected by implementing industry standard security measures.

11.1.2 These areas must have the necessary environmental safety controls in place in the event of fire, floods, earthquakes, power failures, etc.

11.2. Secure Offices

11.2.1 Access to sensitive business and Information and Communication Technology (ICT) areas must be secured and controlled to prevent illegal access.

11.2.2 Appropriate security measures such as security guards, surveillance cameras, access control technologies, etc. must be acquired/implemented to ensure secure access.

11.2.3 The appropriate access control procedures must be implemented to ensure buildings, floors and offices are protected and managed accordingly.

11.2.4 Cameras are required to view access to areas deemed as sensitive or as per CWDM client requirements.

(a) Surveillance footage must be kept for at least ninety (90) days for audit or security investigation purposes.

(b) Audit and security logs must be kept for at least ninety (90) days for audit or security investigation purposes.

(c) System backups must be kept for at least ninety (90) days for audit or security investigation purposes.

12. SECURITY AWARENESS

12.1 The Network Security policy and responsibilities must be communicated to the Heads of Department, ICT Steering Committee, Mayoral Committee, Council and particularly to all resources within the ICT function. Those individuals that have specific roles and responsibilities in terms of this policy must be briefed in detail on the requirements for performance that will be demanded of them during the application of controls, procedures or investigations and systems recovery processes.

12.2 All computer users should be provided with training on the requirements for data and systems security and the responsibilities of each computer user is to uphold the Network Security policy and raise any suspicion of breach of the policy or systems. The objective of this training should be to raise awareness for the need for data and systems security. All new appointments to the municipality must receive training on the Network Security policy during the induction programme.

12.3 Users may not attempt to disable or modify configuration settings to the operating system or any other applications as this may increase security vulnerabilities.

13. ADMINISTRATION AND SUPPORT

The Deputy Director: ICT or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council.

The Network Security Policy shall commence on the date on which it was adopted by Council and shall remain in full force and effective until it is reviewed, revoked or amended by the Council of the Cape Winelands District Municipality.

This Policy shall be called the Cape Winelands District Municipality's Network Security Policy.

13.1. Roles & Responsibilities

13.1.1 Deputy Director: Information & Communication Technology

(a) The Deputy Director: Information & Communication Technology must ensure that all ICT systems are appropriately assessed for security compliance and are adequately secured in accordance with the Network Security Policy.

(b) The Deputy Director: Information & Communication Technology must ensure that ICT security standards are implemented effectively and reviewed on a regular basis.

(c) The Deputy Director: Information & Communication Technology must review all reports of ICT security incidents and respond accordingly.

13.1.2 Senior Network Administrator

(a) The Senior Network Administrator will receive reports of all ICT security incidents for consideration, which must be passed on to the Deputy Director:: Information & Communication Technology for review.

(b) The Senior Network Administrator will assist the Deputy Director:: Information & Communication Technology with the establishment and implementation of ICT security procedures and the communication of said procedures to employees of the Cape Winelands District Municipality (CWDM).

(c) The Senior Network Administrator will ensure that all employees of the Cape Winelands District Municipality (CWDM) are made aware of their ICT security responsibilities through security awareness training.

(d) The Senior Network Administrator will assist the Deputy Director: Information & Communication Technology in monitoring the effectiveness of ICT security within the Cape Winelands District Municipality (CWDM) and will initiate any requested changes to security procedures which become necessary as a result of the monitoring process.

13.1.3 Network Technicians

(a) Network Technicians must monitor ICT security and report ICT security incidents to the Senior Network Administrator.

(b) Network Technicians must ensure that appropriate levels of access are granted to network users.

(c) Network Technicians must ensure that regular backups are taken and stored appropriately off-site.

13.1.4 Network Users

(a) Network Users must comply with the Network Security Policy.

(b) Network Users must notify the Senior Network Administrator or Network Technicians of ICT security breaches that come to their attention.

(c) Network Users must notify the Senior Network Administrator or Network Technicians of all data protection breaches that come to their attention.

(d) May not download or install into any of the drives or devices additional software that has not been approved by the Deputy Director: Information & Communication Technology.

(e) Must not attempt to access data or systems they are not authorized to access and are expected to respect the integrity of Cape Winelands District Municipality's Information and Communication Technology resources.

(f) Are responsible for upholding the confidentiality and integrity of data to which they have access.

13.2. Maintenance & Technical Support (Including System Administration)

13.1.1 Maintenance and technical support must be arranged before the live implementation of infrastructure.

13.1.2 Roles and responsibilities must be clearly defined to ensure effective and efficient support.

13.1.3 Segregation of duties must be applied at all times to prevent unauthorized access or illegal activities being performed by support staff.

13.1.4 Procedures for call-outs and escalation to management must also be clearly documented.

13.1.5 Patches and version upgrades must be done regularly and on time to prevent system vulnerabilities.

13.3. System Monitoring & Reporting

13.3.1 The solution implemented must have monitoring and log reporting capability. Monitoring must be done on a 24 x 7 basis either by the Division: Information and Communication Technology or through an outsourced arrangement. The monitoring arrangement must be reliable and approved by the Manager: Information Technology, with key response and applicable personnel being notified immediately of a system outage or security breach.13.3.2 The system log(s) must be monitored and/or analysed on a regular basis (as deemed necessary and agreed with the Manager: Information Technology) to ensure continuity and availability. Logs must be online accessible for at least one (1) calendar month or as required by government legislation. Archived logs must be available for at least three (3) months or as required by government legislation.

13.3.3 Exceptional reporting must be provided to the Manager: Information Technology regarding policy breaches or irregularities on a monthly basis.

13.4. Configuration Standards & Checklists

13.4.1 Configuration of hardware and software must be done according to approved CWDM standards. When available, checklists must be used to ensure configuration setups are done correctly.

13.4.2 Vulnerability assessments will be done annually to check that security infrastructure is correctly configured. Non-industry standard configurations must be documented and filed.

13.5. 3rd Party Contracts and Service Level Agreement (SLA)

13.5.1 3rd Party contracts (for outsourced arrangements) and SLA's must be documented and in place before any security solution goes live.

13.5.2 Documented approval and sign-off must be obtained from the Manager: Information Technology.

13.6. Systems Access Control

13.6.1 Any systems access required by Users must be approved by the respective Head of Department or delegated Line Manager . Access will only be granted according to job requirement and any change in access

requirements must be approved by the Deputy Director: Information & Communication Technology before being effected.

13.6.2 Passwords must be kept secret and the sharing of passwords will only permitted for support purposes and with the approval from the Deputy Director: Information & Communication Technology .

13.6.3 Passwords for all systems must be strong passwords containing but not limited to:

(a) Not contain the user's account name of parts thereof that exceeds two consecutive characters.(b) Be at least 6 characters long.

(c) Contain characters from e the following four categories:

(i) Upper Case characters (A through Z).

(ii) Lower Case characters (a

through z)

(iii) Base 10 digits (0 through 9).

(iv) Non-alphabetical characters (,: !,@,#,$,%)

13.7. Change Management

13.7.1 Any change to security and ICT infrastructure must follow the Change Control Procedure to effect changes to the current environment. A Change Approval Board (CAB) must be established to review and approve changes to ensure that correct priorities and business impact are appropriately managed.

13.8.1 Internal and external auditors and security consultants will audit or assess any infrastructure or logs at any time in order to ensure that the security policies, standards and procedures are adhered to at all times.

13.8.2 Any vulnerability detected during these audits must be addressed immediately.

13.8. Compliance Monitoring & Audit Reviews

13.8.1 Internal and external auditors and security consultants will audit or assess any infrastructure or logs at any time in order to ensure that

the security policies, standards and procedures are adhered to at all times.

13.8.2 Any vulnerability detected during these audits must be addressed immediately.

14. INCIDENTS AND MONITORING

14.1. Security Incidents

14.1.1 A security incident is any event resulting in a breach of the Information Security policies that affect availability, integrity or confidentiality of information. Examples of this include, but are not limited to events or incidents like cyber attacks, unauthorized access to systems and information, system malfunctions, unauthorized changes to information, program errors, insufficient capacity, loss of data and non compliance to policies and procedures, that compromise information confidentiality, integrity and availability of CWDM information.

14.1.2 All security incidents must be reported to the Deputy : Information & Communication Technology. Security incidents must be logged, investigated and resolved according to the Security Incident Management Process.

14.2. Technical Monitoring

14.2.1 The Network Security Policy is aimed at governing security risks around information. Having the security measurements implemented, it is also important to proactively communicate it through security training, awareness programs and on-going communication. In addition, security measures need to be monitored to ensure compliance and to identify security breaches and respond to it. Such security breaches should be reported to management for action, where relevant.

14.2.2 The solution implemented should have monitoring and log reporting capability. Monitoring should be done by the Division: Information and Communication Technology or through an outsourced arrangement. The monitoring arrangement should be reliable and approved by the Deputy Director: Information & Communication Technology, with key response and applicable personnel being notified immediately of a system outage or security breach.

14.2.3 The system log(s) should be monitored and/or analysed on a regular basis (as deemed necessary and agreed with the Deputy Director: Information

& Communication Technology) to ensure continuity and availability. Logs should be online accessible for at least one (1) calendar month or as required by government legislation.

14.2.4 Offline logs should be stored for at least three (3) months or as required by government legislation. Exception reporting should be provided to the Manager: Information Technology regarding policy breaches or irregularities on a monthly basis.

14.3. Privacy

While CWDM respects the individual's right to privacy as that right is guaranteed under the Constitution of the Republic of South Africa, 1996 and relevant legislation, in the context of electronic communications facilities, which are provided for the CWDM's operational needs, certain restrictions are unavoidable. However, administrators should take note that:

14.3.1 Any personal communication sent, stored or received via the CWDM's electronic communications facilities may only be monitored, intercepted, inspected or refused by duly appointed CWDM representatives as designated by the Municipal Manager.

14.3.2 The typical reasons for such action may include (but are not limited to):

(a) To ensure that the CWDM's electronic communications are not being used in violation of the provisions of the CWDM User & Network Security Policies.

(b) To counteract criminal or fraudulent activities.

(c) To protect the electronic communications facilities from intentional and unintentional damage.

(d) To respond to approved legal proceedings that call for relevant evidence stored electronically.

(e) To conduct investigations in connection with alleged abuse of our electronic communications facilities.