CAPE WINELANDS DISTRICT
MUNICIPALITY • MUNISIPALITEIT • UMASIPALA

NETWORK SECURITY POLICY

POLICY ADOPTED BY COUNCIL ON 25 JULY 2013
AT ITEM C.14.1

POLICY AMENDED BY COUNCIL ON 24 APRIL 2014
AT ITEM C.14.1

TABLE OF CONTENTS

1. INTRODUCTION 3
2. POLICY OBJECTIVE 3
3. TARGET AUDIENCE 3
4. ENVIRONMENT 3
5. VIOLATIONS 3
6. GENERAL 4
7. NETWORK PROTECTION REQUIREMENTS 4
7.1. Firewall (FW) 4
7.2. Cryptography 5
7.3. Remote Login 6
7.4. Wireless Network Access 7
7.5. Content Filtering 7
7.6. Vulnerability Management 8
7.7. Patch Management 9
7.8. Network Point Security 9
7.9. Server and Workstation Lockdown 9
8. SECURE AREAS 10
8.1. Secure Processing (Server & Network Rooms) 10
8.2. Secure Offices 10
9. ADMINISTRATION AND SUPPORT 10
9.1. Roles & Responsibilities 11
9.2. Maintenance & Technical Support (Including System Administration) 12
9.3. System Monitoring & Reporting 12
9.4. Configuration Standards & Checklists 13
9.5. 3rd Party Contracts and Service Level Agreement (SLA) 13
9.6. Systems Access Control 13
9.7. Change Management 14
9.8. Compliance Monitoring & Audit Reviews 14
10. INCIDENTS AND MONITORING 14
10.1. Security Incidents 14
10.2. Technical Monitoring 15
10.3. Privacy 15

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. POLICY OBJECTIVE

2.1 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.

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

2.3 This document purports a layered defence strategy to facilitate the implementation of the minimum security requirements of effective and efficient security solutions.

3. 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.

4. 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.

5. VIOLATIONS

This policy is an extension to the CWDM 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.

6. GENERAL

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

6.2 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.

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

7. 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 Cape Winelands District Municipality (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.

7.1. Firewall (FW)

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.

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

7.1.2 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.

7.1.3 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.

7.1.4 All external connections from the CWDM network to untrusted parties must be done through the firewall.

7.1.5 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.

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

7.1.7 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.

7.1.8 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.

7.2. 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.

7.2.1. 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.

7.2.2. 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 Senior Manager: Strategic Support Services.

7.2.3. 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.

7.3. 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.

7.3.1. External Remote Access

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

7.3.2. 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.

7.4. 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.

7.4.1 WAP's must be hardened and secured.

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

7.4.3 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.

7.5. 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.

7.5.1. 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.

7.5.2. 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.

7.5.3. 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.

7.6. 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.

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

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

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

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

7.7. 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.

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

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

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

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

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

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

7.8. Network Point Security

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

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

7.9. Server and Workstation Lockdown

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

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

8. 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.

8.1. Secure Processing (Server & Network Rooms)

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

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

8.2. Secure Offices

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

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

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

8.2.4 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.

9. ADMINISTRATION AND SUPPORT

The purpose of this section is to document the minimum requirements for effective support and management of security solutions, tools and utilities.

9.1. Roles & Responsibilities

9.1.1 Manager: Information Technology

(a) The Manager: Information 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 Manager: Information Technology must ensure that ICT security standards are implemented effectively and reviewed on a regular basis.

(c) The Manager: Information Technology must review all reports of ICT security incidents and respond accordingly.

9.1.2 Network Support Manager / Network Support Officer

(a) The Network Support Manager / Network Support Officer will receive reports of all ICT security incidents for consideration, which must be passed on to the Manager: Information Technology for review.

(b) The Network Support Manager / Network Support Officer will assist the Manager: Information 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 Network Support Manager / Network Support Officer 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 Network Support Manager / Network Support Officer will assist the Manager: Information 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.

9.1.3 Network Technicians

(a) Network Technicians must monitor ICT security and report ICT security incidents to the Network Support Manager / Network Support Officer.

(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.

9.1.4 Network Users

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

(b) Network Users must notify the Network Support Manager / Network Support Officer or Network Technicians of ICT security breaches that come to their attention.

(c) Network Users must notify the Network Support Manager / Network Support Officer or Network Technicians of all data protection breaches that come to their attention.

9.2. Maintenance & Technical Support (Including System Administration)

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

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

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

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

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

9.3. System Monitoring & Reporting

9.3.1 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.

9.3.2 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.

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

9.4. Configuration Standards & Checklists

9.4.1 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.

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

9.5. 3rd Party Contracts and Service Level Agreement (SLA)

9.5.1 3rd Party contracts (for outsourced arrangements) and SLA's must be documented and in place before any security solution goes live.

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

9.6. Systems Access Control

9.6.1 Any systems access required by Users must be approved by the Senior Manager: Strategic Support Services. Access will only be granted according to job requirement and any change in access requirements must be approved by the Manager: Information Technology before being effected.

9.6.2 Passwords must be kept secret and the sharing of passwords will only permitted for support purposes and with the approval from the Manager: Information Technology.

9.6.3 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 at least 3 of 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 (,: !,@,#,$,%)

9.7. Change Management

9.7.1 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.

9.8. Compliance Monitoring & Audit Reviews

9.8.1 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.

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

10. INCIDENTS AND MONITORING

10.1. Security Incidents

10.1.1 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.

10.1.2 All security incidents must be reported to the Manager: Information Technology. Security incidents must be logged, investigated and resolved according to the Security Incident Management Process.

10.2. Technical Monitoring

10.2.1 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.

10.2.2 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 Manager: Information Technology, with key response and applicable personnel being notified immediately of a system outage or security breach.

10.2.3 The system log(s) should 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 should be online accessible for at least one (1) calendar month or as required by government legislation.

10.2.4 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.

10.3. 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:

10.3.1 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.

10.3.2 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.