FULL COUNCIL RESOLUTION

uMGUNGUNDLOVU
UMASIPALA WESIFUNDA
DISTRICT MUNICIPALITY
DISTRIE MUNISIPALITEIT

Item: 26 (01/11/2019)	ICT POLICIES REVIEW 6/4/P

At its meeting held on 01 November 2019, the Full Council resolved:

1. That the Full Council note the newly developed and reviewed ICT related policies

2. That the Full Council adopt the development and revision of the ICT related policies.

2.1 Tools of Trade for Councillors
2.2 ICT Security Policy
2.3 ICT Usage Policy

CERTIFIED A TRUE EXTRACT OF THE ORIGINAL MINUTES

DR RB NGCOBO
MUNICIPAL MANAGER

INFORMATION COMMUNICATION TECHNOLOGY (ICT) SECURITY POLICY

2019/2020

Adopted by Council: 01 November 2019

Contents

2. Glossary of terms 6

3. EXECUTIVE SUMMARY 8

3.1 INTRODUCTION 8

3.2 OBJECTIVE 8

3.3 SCOPE 8

3.4 POLICY MANAGEMENT & APPROACH 9

4. INFORMATION SYSTEMS SECURITY 9

4.1 OVERVIEW 9

4.2 INFORMATION SECURITY RESPONSIBILITIES 9

4.3 INFORMATION OWNERS 9

4.4 CUSTODIANS OF INFORMATION 10

4.5 INFORMATION USERS 10

4.6 INFORMATION SECURITY SECTION 10

4.7 INTERNAL AUDIT SECTION 10

4.8 EMPLOYEE RESPONSIBILITY 10

4.9 CLASSIFICATION OF INFORMATION SENSITIVITY 10

4.10 DEFAULT CATEGORY 10

4.11 LABELLING 10

4.12 HANDLING INSTRUCTIONS 11

5. ACCESS CONTROL 11

5.1 ACCESS PHILOSOPHY 11

5.2 ACCESS APPROVAL PROCESS 11

5.3 DEFAULT FACILITIES 11

5.4 DEPARTURE FROM THE MUNICIPALITY 11

5.5 UNIQUE USER ID'S 11

5.6 PRIVILEGE DEACTIVATION 11

5.7 USER AUTHENTICATION 11

5.8 MANAGEMENT OF FIXED PASSWORD 12

5.9 CHANGING PASSWORDS 12

6. Bluetooth Baseline Requirements Policy 13

6.1 Overview 13

6.2 Purpose 13

6.3 Scope 13

6.4 Policy 13

6.5 Pins and Pairing 13

6.6 Device Security Settings 13
6.7 Security Audits 13
6.8 Unauthorized Use 13
6.9 User Responsibilities 14
6.10 Policy Compliance 14
6.11 Exceptions 14
6.12 Non-Compliance 14
7. Remote Access Policy 15
7.1 Overview 15
7.2 Purpose 15
7.3 Scope 15
7.4 Policy 15
7.5 Requirements 15
7.6 Policy Compliance 16
7.7 Exceptions 16
7.8 Non-Compliance 16
8. Remote Access Tools Policy 16
8.1 Overview 16
8.2 Purpose 16
8.3 Scope 16
8.4 Policy 17
8.5 Remote Access Tools 17
8.6 Policy Compliance 17
8.7 Exceptions 17
8.8 Non-Compliance 17
9. Router and Switch Security Policy 18
9.1 Purpose 18
9.2 Scope 18
9.3 Policy 18
9.4 Use Accounts 18
9.5 Features and Services 18
9.6 Device logging 19
9.7 Policy Compliance 19
9.8 Exceptions 19
9.9 Non-Compliance 19
10. Wireless Communication Policy 20

10.1 Overview 20
10.2 Purpose 20
10.3 Scope 20
10.4 General Requirements 20
10.5 Lab and Isolated Wireless Device Requirements 20
10.6 Home Wireless Device Requirements 21
10.7 Policy Compliance 21
10.8 Exceptions 21
10.9 Non-Compliance 21
11. Wireless Communication Standard 21
11.1 Purpose 21
11.2 Scope 21
11.3 Wireless Communication Standard Requirements 21
11.4 Lab and Isolated Wireless Device Requirements 22
11.5 Home Wireless Device Requirements 22
11.6 Policy Compliance 22
11.7 Exceptions 22
11.8 Non-Compliance 22
12. Firewall Policy 23
12.1 Purpose 23
12.2 Scope 23
12.3 Policy Statement 23
12.4 Requirements 23
12.5 Operations 23
12.6 Configuration 24
12.7 Audit Compliance 24
12.8 Responsibilities 25
12.9 Change Control 25
12.10 Monitor Stability 25
12.11 Enforcements 25
12.12 Backup 25
12.13 Consequences for Non-Compliance 25

1. Glossary of terms

3-way handshake
Machine A sends a packet with a SYN flag set to Machine B. B acknowledges A's SYN with a SYN/ACK. A acknowledges B's SYN/ACK with an ACK.

Access Control

Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL)
A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service
A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access
Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Matrix
An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.

Account Harvesting
Account Harvesting is the process of collecting all the legitimate account names on a system.

Backdoor
A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

Bandwidth
Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

Banner
A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use.

Cache
Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Cache Cramming

Cache Cramming is the technique of tricking a browser to run cached Java code from the local disk, instead of the internet zone, so it runs with less restrictive permissions.

Cache Poisoning
Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

Call Admission Control (CAC)
The inspection and control all inbound and outbound voice network activity by a voice firewall based on user-defined policies.

Cell
A cell is a unit of data transmitted over an ATM network.

Certificate-Based Authentication
Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.

Daemon
A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

Data Aggregation
Data Aggregation is the ability to get a more complete picture of the information by analyzing several different types of records at once.

Data Custodian
A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

Data Mining

Basic Authentication
Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

Bastion Host
A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

Eavesdropping
Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

Echo Reply
An echo reply is the response a machine that has received an echo request sends over ICMP.

Echo Request
An echo request is an ICMP message sent to a machine to determine if it is online and how long traffic takes to get to it.

Egress Filtering
Filtering outbound traffic.

Emanations Analysis
Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

False Rejects
False Rejects are when an authentication system fails to recognize a valid user.

Fast File System
The first major revision to the Unix file system, providing faster read access and faster (delayed, asynchronous) write access through a disk cache and better file system layout on disk. It uses inodes (pointers) and data blocks.

Fault Line Attacks
Fault Line Attacks use weaknesses between interfaces of systems to exploit gaps in coverage.

File Transfer Protocol (FTP)
A TCP/IP protocol specifying the transfer of text or binary files across the network.

An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

Header
A header is the extra information in a packet that is needed for the protocol stack to process the packet.

Hijack Attack
A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Identity
Identity is whom someone or what something is, for example, the name by which something is known.

Incident
An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

Incident Handling
Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a sixstep process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Incremental Backups
Incremental backups only backup the files that have been modified since the last backup. If dump levels are used, incremental backups only backup files changed since last backup of a lower dump level.

S/Key
A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

Secure Electronic Transactions (SET)
Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

2. EXECUTIVE SUMMARY

2.1 INTRODUCTION

The Information and Communications Technology and Security policy is a formal statement of the rules and guidelines applied by the Municipality which must be adhered to by people utilising and managing the ICT facilities. This policy has been developed in line with the Electronic Communication Security Act, 68 of 2002, the South African Minimum Information Security Standards, and Control Objectives for Information Related Technology (COBIT), ISO 17799, System Administration, Networking and Security Institute (SANS) and Information Technology Infrastructure Library (ITIL).

2.2 OBJECTIVE

The purpose of this document is to formalize an Information and Communications Technology (ICT) Usage and Security Policy, which provides guidelines for introducing and maintaining ICT into the Municipality in a controlled and informed manner, while addressing the key elements of control and security. Those who use the Municipalities ICT facilities are expected to do so responsibly and within normal standards of professional and personal courtesy and conduct.

The purpose of this policy is:

- to inform users and managers of their responsibilities when utilising information assets, as well as for protecting technology and information assets
- to specify the mechanisms through which these requirements must be met
- to provide a baseline from which to acquire, configure and audit computer systems and networks in compliance with the policy
- to minimize disruption to and misuse of the Municipalities ICT infrastructure
- to ensure that the Municipalities resources are used for purposes appropriate to the business mission.
- to define what users may or may not do on the various components of the system infrastructure

Users are hereby informed of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action in line with the Municipalities disciplinary code.

2.3 SCOPE

The policy applies to:

- All ICT infrastructure and systems owned and or used by the Municipality and its users.
- All electronic communications systems and services provided by the Municipality or through third party
- ICT service providers
- All users who gain access to the Municipality‘s infrastructure, systems and ICT facilities
- All records and data in the possession of the employees or other users

2.4 POLICY MANAGEMENT & APPROACH

In order to document a comprehensive ICT policy, all aspects of ICT must be considered and clear rules and guidelines recorded which are appropriate to the culture and risk profile of the Municipality. To define a security policy, a threat analysis must be completed. This is a process where all possible threats to a system are identified and the severity of each threat is measured. This forms the basis of the security policy. Thereafter, once the security policy has been defined, it must be used to decide what security measures must be selected. These are the basic mechanisms used to implement security in a system or organization.

Formulation and maintenance of the policy is the responsibility of the Municipality's ICT Division and the Head of Department under which ICT is aligned to, Awareness of the content and application thereof is the responsibility of the Management of the Municipality.

The ICT Division will be the custodian of all strategic system platforms, communication systems and central computing facilities. The nominated system owners of each Directorate will be the custodians of the strategic applications under their control, while every user will be the custodians of the desktop systems and equipment under their control.

3. INFORMATION SYSTEMS SECURITY

3.1 OVERVIEW

The COMSEC Act and various International Standards and Guidelines requires organizations to develop and implement their Information Systems Security policies to safe guide their data and information systems. This Policy has been developed by the Municipality to conform to the Minimum Information Systems Security Standards of South Africa and to protect the Municipalities ICT assets and Data. This policy also serves as a guideline for users to follow when using the ICT infrastructure so as to minimize the risk of errors, fraud and loss of data. A key aspect of Information Security is to preserve the confidentiality, integrity and availability of an organization's information.

3.2 INFORMATION SECURITY RESPONSIBILITIES

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

3.3 INFORMATION OWNERS

The application and data owners responsibility shall be delegated to the head of that business unit and their responsibly shall be as follows;

- Assign application access rights to existing users and groups within the application.
- Authorize user removal form
- Keep the application administrator passwords in a secure environment

3.4 CUSTODIANS OF INFORMATION

The custodianship of the information shall be dedicated to the Information Technology department. Their responsibility shall be to;

- Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

3.5 INFORMATION USERS

Users will at all times adhere to the Information Security Policy, report all deviations thereof to the Information Security Officer and use the available infrastructure for business purposes only.

3.6 INFORMATION SECURITY SECTION

The appointed ICT Manager provides corporate governance and strategic alliance and empowers ICT STEERING COMMITTEE to enforce this Information Security Policy.

3.7 INTERNAL AUDIT SECTION

The internal audit function shall be to conduct regular security audits in line with ISO 27002 2005 checklist and submit reports to the ICT steering committee for deliberation and action.

3.8 EMPLOYEE RESPONSIBILITY

Ensure that all reasonable precautions are taken to protect business critical data against unauthorized access, especially data on notebooks and portable data storage devices. A locked car in a public area is not a reasonable precaution. It will be the sole responsibility of the user to backup and maintain security of non- business critical data.

3.9 CLASSIFICATION OF INFORMATION SENSITIVITY

The Minimum Information Security Standards (MISS) and ISO 27002 2005 promote the classification of information so that the municipality can be in a position to understand information assets it holds and manage their security appropriately.

3.10 DEFAULT CATEGORY

Information shall be classified in terms of of the MISS, and the following default classification levels shall apply;

- Confidential
- Secret
- Top Secret

Classifications shall also be detailed in the municipality‘s records and archive policy

3.11 LABELLING

Documents shall be labelled in terms of CHAPTER4 (See Annexure A) of the Minimum Information Security Standards of South Africa.

3.12 HANDLING INSTRUCTIONS

Documents shall be handled in terms of CHAPTER 4 Paragraph 3 to 17 (See Annexure A) of the Minimum Information Security Standards of South Africa.

4. ACCESS CONTROL

Access Control is essential to create an optimal information security environment. In terms of the Control of Access to Public Premises Act (Act 53 of 1985) the Municipal Manager (Head of state Organ) is responsible for safeguarding the premises used by or under the Municipality.

4.1 ACCESS PHILOSOPHY

The Municipality from time to time deals with members of the public, business people and other Government workers and foreigners. In order to protect the Municipality against unauthorised access to the premises all areas within the back office environment are in a restricted zone. Areas in the demilitarized shall be accessed during working hours.

4.2 ACCESS APPROVAL PROCESS

Anyone requiring access to the Municipal Premises shall do so by completing a form and submitting the form to the designated Security Officer who will then confirm with the respective Official whether or not to grant access to the person applying for access to the premises. A register shall be kept at all access points exposed to the public of Visitors and vehicles accessing the Municipal Premises.

4.3 DEFAULT FACILITIES

The Municipal Facilities shall be classified as follows:

- Demilitarized Zone – public areas
- Restricted Access – areas accessed by staff members only or by approval
- Authorized Access Only- specialized access only

4.4 DEPARTURE FROM THE MUNICIPALITY

Any Visitor who has been granted access shall sign the visitors register in which they will indicate the date and time when they departed. All visitors' tags shall be returned to the Security Officer upon departure.

4.5 UNIQUE USER ID'S

Every user shall be given a unique user id and password to access the network and an access disc to access the premises.

4.6 PRIVILEGE DEACTIVATION

By default all users shall be deactivated from administrator privileges on the network and on their workstation. Access to information systems and other ICT services shall also be deactivated by default and only given to the user once the relevant approval forms have been signed by the users Head of Department.

4.7 USER AUTHENTICATION

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.

4.8 MANAGEMENT OF FIXED PASSWORD

The responsibility of creating passwords for all users in the Network is limited to only the Information Security Officer or any allocated Information Communication Technology personnel. The passwords are not be accessed by anyone in the municipality unless authorized by the Municipal Manager with the supporting documentation.

4.9 CHANGING PASSWORDS

Users must change passwords after every 40 days. If a user has forgotten his/her password or if the password expires then the user must request the Information Technology Department to change his/her password by completing the relevant forms and submitting them to the ICT division.

5. Bluetooth Baseline Requirements Policy

5.1 Overview

Bluetooth enabled devices are exploding on the Internet at an astonishing rate. At the range of connectivity has increased substantially. Insecure Bluetooth connections can introduce several potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enable devices.

5.2 Purpose

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the UMDM network or UMDM owned devices. The intent of the minimum standard is to ensure enough protection Personally Identifiable Information (PII) and confidential UMDM data.

5.3 Scope

This policy applies to any Bluetooth enabled device that is connected to UMDM network or owned devices.

5.4 Policy

No Bluetooth Device shall be deployed on UMDM equipment that does not meet a minimum of Bluetooth v2.1 specification without written authorization from the IT Team. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

5.5 Pins and Pairing

When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where you PIN can be compromised.

If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, you must refuse the pairing request and report it to IT, through your Help Desk, immediately.

5.6 Device Security Settings

All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.

Use a minimum PIN length of 8. A longer PIN provides more security.

Switch the Bluetooth device to use the hidden mode (non-discoverable)

Only activate Bluetooth only when it is needed.

Ensure device firmware is up to date.

5.7 Security Audits

The IT Team may perform random audits to ensure compliancy with this policy. In the process of performing such audits, IT Team members shall not eavesdrop on any phone conversation.

5.8 Unauthorized Use

The following is a list of unauthorized uses of UMDM owned Bluetooth devices:

Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.

Using UMDM owned Bluetooth equipment on non-UMDM-owned Bluetooth enabled devices.

Unauthorized modification of Bluetooth devices for any purpose.

5.9 User Responsibilities

It is the Bluetooth user's responsibility to comply with this policy. Bluetooth mode must be turned off when not in use.

PII and/or UMDM Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.

Bluetooth users must only access UMDM information systems using approved Bluetooth device hardware, software, solutions, and connections.

Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.

Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.

Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to IT.

5.10 Policy Compliance

The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through's, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.11 Exceptions

Any exception to the policy must be approved by the IT Team in advance.

5.12 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Remote Access Policy

6.1 Overview

Remote access to the corporate network is essential to maintain Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks the best of our ability.

6.2 Purpose

The purpose of this policy is to define rules and requirements for connecting to UDMD's network from any host. These rules and requirements are designed to minimize the potential exposure to UMDM from damages which may result from unauthorized use of UMDM resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical UMDM internal systems, and fines or other financial liabilities incurred as a result of those losses.

6.3 Scope

This policy applies to all UMDM employees, contractors, vendors and agents with a UMDM owned or personally-owned computer or workstation used to connect to the UMDM network. This policy applies to remote access connections used to do work on behalf of UMDM, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to UMDM networks.

6.4 Policy

It is the responsibility of UMDM employees, contractors, vendors and agents with remote access privileges to UMDM's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to UMDM.

General access to the Internet for recreational use through the UMDM network is strictly limited to UMDM employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the UMDM network from a personal computer, Authorized Users are responsible for preventing access to any UMDM computer resources or data by non-Authorized Users. Performance of illegal activities through the UMDM network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

Authorized Users will not use UMDM networks to access the Internet for outside business interests.

For additional information regarding UMDM's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (Intranet portal)

6.5 Requirements

Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

Authorized Users shall protect their login and password, even from family members.

While using a UMDM owned computer to remotely connect to UMDM's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

Use of external resources to conduct UMDM business must be approved in advance by IT and the appropriate business unit manager.

All hosts that are connected to UMDM internal networks via remote access technologies must use the most up-to-date anti-virus software (ESET Endpoint Security v.7.9.v), this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

Personal equipment used to connect to UMDM's networks must meet the requirements of UMDM-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to UMDM Networks.

6.6 Policy Compliance

The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

6.7 Exceptions

Any exception to the policy must be approved by Remote Access Services and the IT Team in advance.

6.8 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Remote Access Tools Policy

7.1 Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include TeamViewer, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the UMDM network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on UMDM computer systems.

7.2 Purpose

This policy defines the requirements for remote access tools used at UMDM

7.3 Scope

This policy applies to all remote access where either end of the communication terminates at a UMDM computer asset

7.4 Policy

All remote access tools used to communicate between UMDM assets and other systems must comply with the following policy requirements.

7.5 Remote Access Tools

UMDM provides mechanisms to collaborate between internal users, with external partners, and from non-UMDM systems. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

All remote access tools or systems that allow communication to UMDM resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.

The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.

Remote access tools must support the UMDM application layer proxy rather than direct connections through the perimeter firewall(s).

Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the UMDM network encryption protocols policy.

All UMDM **antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way**.

All remote access tools must be purchased through the standard UMDM procurement process, and the information technology group must approve the purchase.

7.6 Policy Compliance

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through's, monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

7.7 Exceptions

Any exception to the policy must be approved by the IT Team in advance.

7.8 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. Router and Switch Security Policy

8.1 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of UMDM.

8.2 Scope

All employees, contractors, consultants, temporary and other workers at UMDM and its subsidiaries must adhere to this policy. All routers and switches connected to UMDM production networks are affected.

8.3 Policy

Every router must meet the following configuration standards:

8.4 Use Accounts

- No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
- The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

8.5 Features and Services

The following services or features must be disabled:

- IP directed broadcasts
- Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
- TCP small services
- UDP small services
- All source routing and switching
- All web services running on router
- UMDM discovery protocol on Internet connected interfaces
- Telnet, FTP, and HTTP services
- Auto-configuration
- The following services should be disabled unless a business justification is provided:
- UMDM discovery protocol and other discovery protocols
- Dynamic trunking
- Scripting environments, such as the TCL shell

The following services must be configured:

- Password-encryption
- NTP configured to a corporate standard source

All routing updates shall be done using secure routing updates.

Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

Access control lists for transiting the device are to be added as business needs arise.

The router must be included in the corporate enterprise management system with a designated point of contact.

Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

The corporate router configuration standard will define the category of sensitive routing and switching devices and require additional services or configuration on sensitive devices including, IP access list accounting.

8.6 Device logging

Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped

Router console and modem access must be restricted by additional security controls

8.7 Policy Compliance

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.8 Exceptions

Any exception to the policy must be approved by the IT team in advance.

8.9 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9. Wireless Communication Policy

9.1 Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

9.2 Purpose

The purpose of this policy is to secure and protect the information assets owned by the District. UMDM provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. UMDM grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to UMDM network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy or are granted an exception by the Information Technology Department are approved for connectivity to a UMDM network.

9.3 Scope

All employees, contractors, consultants, temporary and other workers at UMDM including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of UMDM must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a UMDM network or reside on a UMDM site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

9.4 General Requirements

All wireless infrastructure devices that reside at a UMDM site and connect to a UMDM network, or provide access to information classified as UMDM Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use UMDM approved authentication protocols and infrastructure.
- Use UMDM approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

9.5 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to UMDM Confidential or above, must adhere to section 6.4 above. Lab and isolated wireless devices that do not provide general network connectivity to the UMDM network must;

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

9.6 Home Wireless Device Requirements

Wireless infrastructure devices that provide direct access to the UMDM corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the UMDM corporate network. Access to the UMDM corporate network through this device must use standard remote access authentication.

9.7 Policy Compliance

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

9.8 Exceptions

Any exception to the policy must be approved by the IT team in advance.

9.9 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10. Wireless Communication Standard

10.1 Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a UMDM network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the IT Team are approved for connectivity to a UMDM network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (IT) approved support organization. Lab network devices must comply with the Lab Security Policy.

10.2 Scope

All employees, contractors, consultants, temporary and other workers at UMDM and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of UMDM must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

IT must approve exceptions to this standard in advance.

10.3 Wireless Communication Standard Requirements

All wireless infrastructure devices that connect to a UMDM network or provide access to UMDM Confidential, UMDM Highly Confidential, or UMDM Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.

- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

10.4 Lab and Isolated Wireless Device Requirements

Lab device Service Set Identifier (SSID) must be different from UMDM production device SSID.

Broadcast of lab device SSID must be disabled.

10.5 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a UMDM network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

10.6 Policy Compliance

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

10.7 Exceptions

Any exception to the policy must be approved by the IT Team in advance.

10.8 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11. Firewall Policy

11.1 Purpose

The purpose of this ICT Firewall Policy is to define which traffic is allowed or blocked, thus define the Network devices and services that are allowed or blocked from sending or receiving from the Internet. To define standards for provisioning security devices owned by the uMgungundlovu District Municipality. To prevent exploitation of insecure services, restrict inbound/outbound traffic from unregistered devices, control inbound/outbound access to/from specific services or devices and monitor traffic volumes.

11.2 Scope

This policy defines the essential rules regarding the management and maintenance of Firewall at uMgungundlovu District Municipality and it applies to all users that use computer and the network of the uMgungundlovu District Municipality.

11.3 Policy Statement

UMgungundlovu District Municipality operates perimeter firewalls between the Internets, municipal network as well the Customer Care Centers in order to establish a security environment for the municipality's Information Technology resources. UMgungundlovu District Municipality perimeter firewalls are key components of the overall municipal's Network Security Architecture. This ICT Policy governs how the perimeter Firewalls will filter Internet traffic to mitigate risk and possible losses associated with security threats to the network information systems.

11.4 Requirements

- The Firewall shall control all traffic entering and leaving the municipal internal network.
- UMgungundlovu District Municipality Firewall shall block all incoming and outgoing traffic by default.
- Only authorized incoming and outgoing traffic shall be allowed to pass through the Firewall.
- Traffic with invalid sources or destination addresses shall always be block.
- Traffic from outside the network containing broadcast addresses that are directed to inside the network shall be block.
- Social media access shall be blocked on everyone in the municipality with the exception to the Communication department.
- All Customer Care Centre shall gain access to the main Office via a VPN that shall be tunneled from a firewall on their site to the main firewall.
- CCC's shall have the same access to the internet like the users at the head office.
- CCC's shall access all municipal applications via the Firewall point to point connection.

11.5 Operations

There shall only be one administrator of all the Firewalls within the municipality. In the absence of the administrator, there shall be a temporal account created for the person who shall be left in charge of the Firewall.

Access to the Firewall shall be tightly controlled. Only the Firewall administrator is allowed to have a user account on the Firewall. Firewall administrator shall have a personal account.

All changes to Firewall access rules shall be made through a single approved interface. The firewall shall have a trusted path for its management e.g. physically secure dedicated management process with password-based identification and authentication system.

Only the administrator shall make changes to the Firewall access rules, software, hardware or configuration. All changes shall be as a result of a request recorded in a Change Management System although emergency modifications can be requested by phone, with follow up email and change request. Only authorized personnel must be able to implement the changes and an audit log must be retained as per the Municipality's ICT Change Management Policy.

Logging and audit facilities provided by the Firewall shall be fully utilized. All significant traffic through the Firewall shall be logged. The Firewall should provide sufficient audit capacity to detect breaches of the Firewall's security and attempted network intrusions and should report in real time. The Firewall Administrator shall examine the logs on a regular basis and also set up mechanism to respond to alarms.

11.6 Configuration

The perimeter Firewall shall be configured to deny any services unless it is expressly permitted. If there are no rules defined for the municipal network address, then traffic to or from that address shall be denied. Access to the municipal network shall be blocked during the start–up procedure of the Firewall.

The Firewall operating system shall be configured for maximum security, this including disabling of any unused service.

The initial build and configuration of the Firewall shall be fully documented. This provides a baseline description of the Firewall to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

Security shall not be compromised by the failure of any hardware component. If any component of the Firewall fails, the default response will be to immediately prevent any further access, both outbound and inbound. A Firewall component is any piece of hardware or software that is an integral part of the Firewall system. A hardware failure occurs when equipment malfunctions or switched off. A software failure can occur for many reasons e.g. bad maintenance of the rules database on the Firewall or software which is incorrectly installed or upgraded.

There shall be regular reviews to validate that the Firewall system meets the need of the business regarding information security. The configuration of the Firewall shall be regularly checked to ensure they still match the business requirements regarding the security. The Firewall must be regularly test for vulnerabilities.

11.7 Audit Compliance

Regular testing of the Firewall shall be carried out. The Firewall shall be tested for:

Configuration errors that may represent a weakness that can be exploited by those hostile intent.

Consistency of the Firewall rule set.

Secure base system implementation.

The Firewall shall have an alarm capability and supporting procedures. When an agreed specified event occurs, an alarm in a form of sms or email shall be sent to the team. Documented procedure shall exist to permit an efficient response to such Firewall security alarms and incidents. In the event that the Firewall itself is the subject of malicious attempts to penetrate it and the Firewall has the capability, delivery of services be terminated rather than permit uncontrolled access to the municipal network.

There shall be an active auditing/logging regime to permit analysis of Firewall activity both during and after a security event. An audit trail is vital in determining if there are attempts to circumvent the Firewall security. Audit trails must be protected against loss or unauthorized modification. The Firewall must be able to provide logging of specific traffic when suspicious activity is detected.

11.8 Responsibilities

ICT Division will be the sole responsible entity for putting in place firewalls and the management thereof. The monitoring will be done by the ICT Division reported to the ICT Steering Committee if any attempts are detected and any activity of misuse of the Internet by users.

11.9 Change Control

With any Firewall it is very important to have change control. When rules are introduced there should be a well-defined method for documenting these and in the case of temporary rules, the removal date for the rule should be added in a comment field. The only way of checking if the Firewall is actually enforcing the agreed policy is to either verify it with an Intrusion Detection System, or do a manual verification using a penetration test or a Firewall reviewed by third party.

11.10 Monitor Stability

A Firewall is like any other infrastructure component and should be managed as such. IT should be monitored for availability to ensure maximum uptime. If a Firewall isn't stabile, people will find ways of avoiding the Firewall that leads to low level of security.

11.11 Enforcements

ICT Division is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

11.12 Backup

Backups shall be performed once a quarter and stored on the backup NAS or server. Quarterly backups should be stored on an offsite backup location. Backups should also be performed before and after a change is made to the configuration. UMgungundlovu District Municipality shall also have a backup firewall in reserve should there be a malfunction to the existing backup.

11.13 Consequences for Non-Compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.