AMAJUBA DISTRICT MUNICIPALITY (ADM)

ICT SECURITY POLICY

VERSION 1.0

WONDER MADI: ADM ACTO
wonderm@majuba.gov.za

Document Control

ITEM	VALUE
Date:	25-05-2023
Author/s:	Wonder Madi, Mark Durham.
Security Level:	Client confidential
Document Name:	ADM ICT Security Policy
Document Stored As:	ADM ICT Security Policy v1.docx
Special Instructions:	None

Revision Control

REVISION	DATED	REVISED BY	DESCRIPTION OF MAJOR CHANGES
1.0	25-05-2023	Wonder Madi, Mark Durham.	Final Document

Abbreviations

Abbreviation	Term
CGICT	Corporate Governance of ICT
CGICTPF	Corporate Governance of ICT Policy Framework
COGTA	Department for Co-Operative Governance and Traditional Affairs
DPSA	Department of Public Service Administration
EXCO	Executive Committee
GICT	Governance of ICT
GITO	Government Information Technology Officer
ICT	Information and Communications Technology
IDP	Integrated Development Plan

MANCO	Management Committee
MTEF	Medium Term Expenditure Framework

Document No.	ADM/ICT/006
Version No	1.0
Date Approved by Council	30 June 2023

Signature: _____

Name: _____

ON BEHALF OF THE MUNICIPAL COUNCIL

Effective date: 25-05-2023
Revised Date: 30-06-2023

Location: IT Policies, Forms and Information

Controlled Document

This is a controlled document and may be subject to change at any time with the approval of Council.

Owner: Chief Technology Officer

Status: Final Document

Revision History Release No.	**Date**	**Author**	**Revision Description**
V1.0	2023/06/30	Wonder Madi, Mark Durham.	Final Document

Introduction

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's IT systems, data and infrastructure are protected from risks such as unauthorised access (see IT User Access Management Policy for further detail), manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

Objective of the policy

The objective of the policy is to reduce the risk of harm that can be caused to the Municipality's IT systems, information and infrastructure. This policy also seeks to outline the acceptable use of IT resources by officials and 3rd party service providers, to ensure that the investment in modern technology is applied to the best advantage of the Municipality.

This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of the Municipality's strategic goals and objectives.

Aim

The aim of this policy is to ensure that the Municipality conforms to a standard set of security controls for information security in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of Information Security are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

Scope

This IT Security Controls Policy has been developed to guide and assist the municipality to be aligned with best practice IT Security Controls. This policy recognises that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of information security.

The policy applies to everyone in the Municipality, including its third-party service providers and consultants.

This policy is regarded as being critical to the security of IT systems of the Municipality.

Aspects relating to user access, server security and data backup are covered in the IT User Access Management, and the IT Data Backup and Recovery policies

Administration of Policy

The ICT Manager or delegated authority is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by Council.

Protection of Policy

The Municipal Systems Act, Act No. 32 of 2000, Schedule 1: Code of Conduct for Councillors and Schedule 2: Code of Conduct for Municipal Staff Members require Councillors and Officials to employ a strict level of self-discipline in order to prevent communication of sensitive or classified information.

Councillors and Officials may not disclose any privileged or confidential information to an unauthorised person.

All Municipal data must be classified in accordance with the Minimum Information Security Standards, s approved by Cabinet in 1996. Therefore all official matters requiring the application of security measures must be classified either as "Restricted" or "Confidential". By default, Municipal data has been classified as Restricted

Classification Description Restricted Information that may be used to hamper Municipal activities. Confidential Information that may be used harm the objectives and functions of the Municipality.

Access to classified information is determined either by the level of security clearance, or if the information is required in the execution of their duties.

Officials, in conjunction with the ICT Manager, must ensure that classified information receives adequate protection to prevent compromise.

Officials who generate sensitive information are responsible for determining the information classification levels. This responsibility includes the labelling of classified documents.

The Minimum Information Security Standards Chapter 6, Section 1 requires that a declaration of secrecy must be made on an official form during the appointment process for any government post.

Protection of public Records

The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions

The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the Municipality.

The ICT Manager must work with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

Information security plays an important role in records management as a means to protect the integrity and confidentiality of public records. The ICT Manager must ensure that systems used for records management of electronic public records and emails are configured and managed as follows:

- Systems must capture appropriate metadata (background and technical information about the data);
- The systems must establish an audit trail to log all attempts to alter or edit electronic records and their metadata;
- The system must protect the integrity of records until they have reached their approved retention. Integrity of records can be accomplished through procedures such as backup test restores, media testing, data migration controls and capturing the required audit trails;
- Access controls must protect records against unauthorized access and tampering;
- Access controls must prevent removal of data from premises without the explicit permission of the ICT Manager;
- Systems must be free from viruses;
- The system must ensure that electronic records, that have to be legally admissible in court and carry evidential weight, are protected to ensure that they are authentic, not altered or tampered with, auditable and produced in systems which utilise security measures to ensure their integrity.
- Access to server rooms and storage areas for electronic records media must be restricted to ICT staff with specific duties regarding the maintenance of the hardware, software and media.

- Systems technical manuals and systems procedures manuals must be designed for each system.
- A systems technical manual includes information regarding the hardware, software and network elements that comprise the electronic record keeping system and how they interact. Details of all changes to a system must also be documented.
- A system procedures manual includes all procedures relating to the operation and use of the system, including input to, operation of and output from the system. A systems procedures manual should be updated when new releases force new procedures.
- The ICT Manager must ensure that the suitability of new system for records management is assessed during its design phase. The Records Manager must be involved during the design specification.

Protection of Personal Information

The Bill of Rights in the Constitution states that the public has a right to privacy, as well as a right to access personal information held by the Municipality.

The Promotion of Access to Information Act, Act No. 2 of 2000, gives effect to the right to access personal information held by the Municipality and must be complied with.

The Protection of Personal Information Act, Act No. 4 of 2013, gives effect to the right to privacy. The Act requires that the Information Officer of the Municipality ensure that personal information is lawfully obtained and processed.

The ICT Manager and Officials must work together to ensure the following with respect to personal information (only key points of the Act included):

- Identify the systems and locations where personal information can be found;
- Ensure that Municipal policies, in particular those that deal with information security, are applied to the systems and locations where personal information is collected, processed and disposed of;

Put in place business process controls to ensure that personal information is collected lawfully, is complete and accurate, and updated where necessary;

- Dispose of excessive personal information, after consultation with the Records Manager;
- Put in place structures and systems to allow the access of persons to their personal information stored by the Municipality. The requester may request to have their personal information deleted or corrected if it is incorrect or obtained unlawfully; and
- Ensure that systems do not use personal information as the sole basis to decide legal consequences for a person or group of persons (referred to as “automated decision making”).

The Protection of Personal Information Act, No. 4 of 2013, Section 6, contains certain general exceptions where the Act does not apply e.g. the processing of personal information for national security, defence, public safety, law enforcement or for the judicial functions of a court.

The Protection of Personal Information Act, No. 4 of 2013 prohibits the processing of certain categories of special personal information. The general exception is where a competent person (e.g. in the case of children) have given consent, or if an exception applies. Examples are shown hereunder (refer to the Act for further detail):

Protection of Personal Information Act, No. 4 of 2013

The following personal information are not regarded as special personal information and must be protected in terms of the general rules for the protection of personal information:

Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views, preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears next to other personal information or if the name itself would reveal personal information about the person.

The Promotion of Access to Information Act, Act No. 2 of 2000, prohibits the disclosure of certain types of information held by the Municipality, including, but not limited to personal information. These include:

- Commercial information of a third party;
- Information that falls under a confidentiality agreement;
- Information that is likely to endanger the safety of individuals if it is made public;
- Police dockets in bail proceedings;
- Records privileged from production in legal proceedings
- Research information of a third party;
- Security information about a building, structure or system;
- Methods, techniques, procedures or guidelines for law enforcement and legal proceedings;
- Information that will prejudice the defence, security and international relations of the Republic;
- Information that will jeopardise the economic interests and financial welfare of the Republic and commercial activities of the Municipality;
- Research information of the Municipality; and
- Information about the operations of the Municipality.

The Promotion of Access to Information Act, Act No. 2 of 2000, require that information relating to public safety, environmental risk, or a substantial contravention of, or failure to comply with the law, be disclosed immediately.

Protection of Records to Preserve Legality

The Electronic Communications and Transactions Act, Act. No. 25 of 2002, prescribes information security controls to preserve the evidential weight of electronic records and e-mails.

The evidential weight of electronic records and e-mails is a continuum, where the weight of the evidence increases with the number of information security controls applied. The following lists examples of such specific information security controls:

- Restrict access to records
- Encrypt records
- Store records on write once, read many times, media
- Apply records management principles
- Store records in a database management system
- Apply change control to the records management system
- Backup data
- Use digital certificates to confirm the identities of senders and receivers of messages

General Control Environment

To ensure reliability of ICT services and to comply with legislation, all Municipal systems and infrastructure must be protected with physical and logical security measures to prevent unauthorised access to Municipal data.

Physical and logical security is a layered approach that extends to user access, application security, physical security, database security, operating system security and network security.

Refer to the ICT User Access Management Policy and the ICT Operating System Security Controls Policy for the requirements relating to user access, applications and operating system security.

Physical Security

The ICT Manager must take reasonable steps to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery. ICT hardware under control of the ICT function must be hosted in server rooms or lockable cabinets. Server rooms must be of solid construction and locked at all times.

The ICT department must retain an access control list for the server room. Access must be reviewed quarterly by the ICT Manager.

All server rooms must be equipped with appropriate controls, as detailed in the IT Facilities Management Policy.

No ICT equipment may be removed from the server room or offices without prior authorisation from the ICT Manager.

Officials of the Municipality must be made aware of the acceptable use of ICT hardware.

All hardware owned by the Municipality must be returned by employees and service providers when no longer needed or on termination of their contract.

All data and software on hardware must be erased prior to disposal or re-use.

Any hardware that carry data that can be carried off-site (e.g. laptop computers, removable hard disks, flash drives etc.) must be protected with encryption.

ICT hardware and software must be standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the Municipality.

The location used to store backup data media, must be protected with appropriate security and environmental management measures.

Database Security

Where applicable, the IT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to IT staff who need this access. Officials who use applications may not have these rights to the application's databases.

The IT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.

The IT Steering Committee must approve all instances where Officials have edit or execute access to databases.

The IT Manager must review database rights and permissions on a quarterly basis. Excessive rights and permissions must be removed.

Network Security

The IT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.

The IT Manager must implement a firewall between the Municipal network and other networks.

The IT Manager must limit administrator access to the firewall and user accounts must adhere to the User Access Policy.

The IT Manager must check and install firewall upgrades and patches on a weekly basis. An obsolete firewall (one that is not supported by the vendor any longer and / or has known security vulnerabilities) must be replaced.

The IT Manager must document the firewall rulesets and configuration settings. The rulesets and configuration settings must be reviewed quarterly to ensure that it remains current (i.e. remove unused services) and that services that expose the Municipality to security risk are reviewed continuously.

The IT Manager must configure the firewall to block all incoming ports, unless the service is required to connect to a server on the internal network (e.g. port 80 and port 443 for web servers). When an incoming port is allowed, the service may only connect to the specific servers on the internal network. Internal IP addresses may not be visible outside of the internal network.

The IT Architectural Committee must approve all open incoming ports. The IT Steering Committee must only approve requests that are absolutely necessary and with consideration of the associated security risks.

The system administrators must set the firewall to block intrusion attempts and to alert the IT Manager when additional action needs to be taken. The IT Manager must raise an incident and deal with the root causes of the event.

The IT department must scan the entire network with security software on a regular basis to detect security vulnerabilities. The scans may be performed from the Internet, as well as from the internal network.

Officials and the IT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.

System administrators must install appropriate endpoint security software on laptops and personal computers. Officials may not disable these applications. Officials must choose to deny a specific address when prompted by the endpoint security software, unless approved by IT.

E-mail and Internet

The IT Manager must make all users aware of the safe and responsible use of email and Internet services. E-mail and Internet should only be used for official use. Personal usage can be permitted if it does not interfere with job functions. E-mail and Internet may not be used for any illegal or offensive activities.

Officials and the IT department may not use Internet cloud services (e.g. Google drive, Gmail, Dropbox etc.) for official purposes unless approved by the IT Steering Committee.

Wireless Networks

System administrators must configure all wireless networks to the following standard:

- WPA2 security protocol or better;
- Password strength of at least 10 characters with a combination of alpha-numeric characters and symbols;
- The latest firmware must be installed; and
- Default system usernames and passwords must be removed.

Officials may not establish wireless networks attached to the internal network without the consent of the IT Manager. All wireless networks must adhere to the secure configuration standard.

Mobile Devices and own Hardware (BYOD)

The IT Manager must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.

The IT team must ensure that all mobile devices must be protected with a PIN.

Transfer Information

The IT Manager must ensure that classified information may only be transmitted over external networks using encryption.

Officials may not use personal storage devices (e.g. USB memory sticks or portable hard drives) to store Municipal data. When required for official purposes, and the data is of a confidential nature, these devices must be encrypted by the IT Manager.

Monitoring

The Municipal Manager authorises the monitoring of Municipal systems by the IT Manager.

Municipal officials must be made aware that the network is being monitored to ensure network security, to track the performance of the network and systems, and to protect the network from security threats.

If users give their written consent, any e-mail, Internet and other network service may be monitored. A signed acceptable user agreement is required in order to achieve this consent.

Security Incident Management

All Municipal users must report actual or suspected security breaches or security weaknesses to the IT Manager or the delegated authority.

The IT Manager must record all information regarding security incidents. The IT Manager must review all the information security incidents on a quarterly basis to ensure that the root causes of the problems are addressed.

Investigations into security incidents may only be carried out by the IT Manager or a nominated person.

The Protection of Personal Information Act, Act No. 4 of 2013 prescribe that the Regular and the person affected by the breach must be notified in the event of a breach of personal information.

Change Control

All changes to Municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable IT service delivery to the Municipality, without impacting the stability and integrity of the changed environment.

Change Control requirements are detailed in the IT Change Control Policy.

Software Authorization and Licensing

The IT Manager must retain a record of all licenses owned by the Municipality

The IT Manager must scan all IT resources on an annual basis to verify that only authorised software is installed.

The IT Steering Committee must approve all software being used in the Municipality. An approved software list must be maintained by the IT Manager and approved by the IT Steering Committee.

The IT Steering Committee may only authorise software from known, reputable sources to reduce the likelihood of introducing errors or security risks into the environment.

Officials may not install or change the software on their computer

Breach of Policy

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity.

The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and IT services;
- Disciplinary action in accordance with the Municipal policy; or
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
- Punitive recourse against a service provider in terms of the contract.

Reference Documentation

Refer to ADM IT Policies, Forms and Information stored on ADM report repository

SOURCE.....	Nhlonipho Mdakane, Mark Durham.
REPLACING.....	New
REVISION No.	Version 1.0
Signature of Head of Department.....	