# INFORMATION TECHNOLOGY POLICY

# JOHN TAOLO GAETSEWE DISTRICT MUNICIPALITY

| | |
|---|---|
| **Council Resolution:** 6.1.27/06/2023 | **Approved Date:** 27/06/2023 |
| **Effective Date:** 1 July 2023 | **Review Date:** As and when required |

**MUNICIPAL MANAGER**

**SPEAKER**

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

# JOHN TAOLO GAETSEWE DISTRICT MUNICIPALITY

# INFORMATION TECHNOLOGY POLICY

## 2023-2024

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

## Document Control

| | |
|---|---|
| **Organization** | John Taolo Gaetsewe District Municipality |
| **Title** | Information Technology Policy |
| **Author** | Senior IT Officer |
| **Filename** | JTGDM IT Policy |
| **Owner** | HOD Corporate Services |
| **Subject** | IT policy |
| **Policy Review date** | Annually |

## Document Approvals

This document requires the following approvals:

| **Council/Management Approval** | **Name** | **Date** |
|---|---|---|
| Municipal Manager | | |
| Council Speaker | | |

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

**TABLE OF CONTENTS** **PAGE**

## DEFINITIONS AND ABBREVIATIONS

### Definitions

**"Authentication"** - Authentication is the process of verifying the identity of a user or application with the system, typically via a password. When users and applications use unique passwords that are difficult to guess and that are changed regularly, a system can be relatively certain that the user is who they claim to be, and can grant access as required.

**"Access Control"** - Access control is the process of granting users and applications the level of information and resources required to support their job or a business function.

**"Access control card holder"** - Any person officially issued with an access control card to allow access to designated John Taolo Gaetsewe District Municipality areas, buildings and other facilities.

**"Access role"** - An access role is the set of systems access required to perform a job function. Therefore, the access role for a given job function is that level of access which allows the user or application to perform his/her job function.

**"Incident"** - Any adverse event, suspected event or vulnerability that could pose a threat to some aspect of computer security (i.e. loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability of services and/or data)

**"Restore"** - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

**"RBAC"** - Role Based Access Control, access to any system or application is assigned based on the functional responsibilities or roles of that person or system.

**"DMZ" (De-militarized Zone)** - A network segment external to the corporate production network.

**"Backup"** - The process of *copying* active files from online disk storage to tape so that files may be restored to disk in the event of damage to or loss of data.

**"Archive"** - The process of *moving* inactive files from online disk storage to tape, i.e. deleting the files from disk after copying them, in order to release online storage for re-use.

**"User/s"** - Any person/s that has access to and makes use of a computing device

**"Least Privilege"** - Minimum privileges and rights required by a person or system in order to allow that person or system effective execution of the functions.

**"Patch"** - Means a piece of software designed to fix problems with or update a computer program or its supporting data.

**"Trojan"** - Means a class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions.

**"Virus"** - Means a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

**"Worm"** - means a self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

**"Windows Server Update Services" (WSUS)** - Means a free patch management tool available to Windows Server administrators. WSUS allows administrators to authorize/publish and distribute updates within a network.

**"Push Technology"** - Means client/server applications used to send data to a client without the client requesting it.

**"Server"** - Means a system (software and suitable computer hardware) that responds to requests across a computer network to provide, or help to provide, a network service.

**"Workstation"** - is a microcomputer designed primarily to be used by one person at a time, they are commonly connected to a local area network and run user operating systems and applications.

**"Information Technology"** - Means all aspects of technology that are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource.

**"Local Area Network"** - Means a high-speed communication infrastructure that enables users to share resources such as hardware, software, data or Wide Area Network (WAN) communication in a cost-effective manner.

**Abbreviations**

| | | |
|---|---|---|
| JTGDM | : | John Taolo Gaetsewe District Municipality |
| IP Address | : | Internet Protocol Address |
| DNS | : | Domain Name Systems |
| DHCP | : | Dynamic Host Configuration Protocol |
| LAN | : | Local Area Network |
| WAN | : | Wide Area Network |
| ITU | : | Information Technology Unit |
| MB | : | Mega Bytes |



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

## 1. INTRODUCTION

1.1 The Information Technology Management in John Taolo Gaetsewe DM – IT, is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded between Information Resources infrastructure, the need for a strong change management process is therefore essential.

1.2 JTGDM is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. JTGDM has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common system vulnerability threats to the systems within this scope.

1.3 From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

## 2. PURPOSE

2.1 Information is a vital municipal asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth requirements for incorporation of information security practices into daily usage of municipality information systems

2.2 To provide guidelines that allow for the unique identification of each user who is granted access to any system on the JTGDM network in order to enhance the confidentiality and integrity of data and associated information of the John Taolo Gaetsewe District Municipality.

2.3 To reduce the administrative load relating to the management of security related incidents.

2.4 To provide all members of staff and councilors with access to E-mail.

2.5 Every user will be provided with their own e-mail address, and have access to external e-mail communications.

2.6 To outline the process of maintaining the IT strategic plan as well as the purpose of the plan.

2.7 To clarify the process and authority of the IT steering committee.

2.8 To define policy for backup of computer systems housed within the server room.

2.9 To describe the procedure for requesting changes on JTGDM IT infrastructure. This document describes procedures used by the ITU to achieve these goals.

2.10 To manage changes in a rational and predictable manner so that staff and clients can plan accordingly.

2.11 The co-ordination of planned replacement of IT equipment centrally coordinated via Information Technology Unit.

2.12 Consistent provision of IT Equipment within the municipality to meet the user`s needs.

2.13 The replacement of IT Equipment on current utilization and planned developments.

2.14 To provide the means for the disposal of redundant or obsolete IT Equipment.

2.15 To eradicate theft or loss of IT Equipment.

2.16. To describe the requirements for maintaining up-to-date operating system security patches on all JTGDM owned and managed workstations and servers.

2.17 To enable the municipality to control changes and additions and access to the Information Technology environment, the completion of a change request form is required.

## 3. POLICY OBJECTIVES

3.1 This policy is designed to protect the organization's information resources against intrusion and destruction by viruses and other malware.

3.2 Effective use of municipality IT resources: This policy is designed to support the implementation of internal inventory control procedures, IT equipment replacement method, asset management processes and general tracking of JTGDM IT assets/equipment.

3.3 Provide complete, accurate financial audit capabilities for technology assets as needed by the Budget and Treasury Office, Internal Audit, or third-party auditors.

3.4 Provide the Municipality with information to track IT assets/equipment that have been reported stolen, lost or missing.

3.5 Ensure that IT initiatives are aligned with business objectives.

3.6 Derive specific objectives from the strategy.

3.7 Prioritize IT initiatives and develop proper project plans.

3.8 To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

3.9 To establish prudent and acceptable practices regarding the use of e-mail.

3.10 To educate individuals who may use e-mail with respect to their responsibilities associated with such use.

3.11 To specify allocations of computers in the Municipality.

3.12 To guide the IT section on how to deal with private equipment.

3.13 To guide users on the usage of the IT systems.

3.14 To guide users on the security standards of the IT resources.

3.15 To specify standards that the Municipality adheres to.

3.16 To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.

3.17 To establish prudent and acceptable practices regarding the use of e-mail.

3.18 To educate individuals who may use e-mail with respect to their responsibilities associated with such use.

3.19 To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.

3.20 To establish prudent and acceptable practices regarding the use of the internet.

3.21 To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

## 4. SCOPE

4.1 This policy applies to all entities including but not limited to officials, politicians, contractors, service providers, permanent and temporary workers who may require access to John Taolo Gaetsewe District Municipality's computer systems and applications.

4.2 This policy applies to all systems that are in official use in John Taolo Gaetsewe District Municipality regardless of the purpose of the system or the department which it primarily serves.

4.3 The policy covers the entire municipality's requirement with regards to access to any IT equipment, application and/or electronic mail connected to the local LAN and/or WAN and is applicable to all computer users connected to the network.

4.4 This policy applies to all IT Equipment of JTGDM which are used within JTGDM.

4.5 This policy applies to workstations and servers owned or managed by JTGDM. This includes systems that contain company or customer data owned or managed by JTGDM regardless of location.

## 5. LEGAL FRAMEWORK

5.1 The Constitution of the SA, Act 108 of 1996

5.2 Municipal Finance Management Act 56 of 2003

5.3 Local Government Municipal Structure Act 117 0f 1998

5.4 Local Government Municipal Systems Act 32 of 2000



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

5.5 Minimum Information Security Standards (MISS). The purpose of the MISS is to establish policy frameworks for general guidance of Information Technology practices to ensure that IT as strategic resource is utilized fully and cost effectively.

5.6 The State Information Technology Agency (SITA) Act, as amended.

5.7 Electronic Communication Transaction Act, 2002.

5.8 The Protection of Information 84 Act of 1982.

5.9 The Promotion of Access to Information Act.

5.10 The National Archives Act 43 of 1996.

## 6. POLICY CONTENTS AND PROCEDURES

### 6.1 User Management and IT Infrastructure Access Control

#### 6.1.1 APPLICATION NEW USER REGISTRATION

6.1.1.1 Any application (E-mail, Network, FMS, Sage 300 people, Sage Accounting or other server-based business applications) will only be available to users connected to the municipal network. In order to be connected to the municipal network, the relevant user must:

6.1.1.2 Fill out the form contained in Appendix A.

6.1.1.3 Obtain approval from his/her Head of Department

6.1.1.4 Obtain approval from the relevant owner of the application.

6.1.1.5 Forward approved form to the ITU for approval & implementation.

6.1.1.6 The form is then filed for future reference.

### 6.1.2 USER DEREGISTRATION

Access rights of users who have left the company should immediately be removed, procedure in place:

6.1.2.1 IT should be informed in writing from HR Department regarding employer termination.

6.1.2.2 User must complete access Removal form and signed off by Supervisor and Head of Department

6.1.2.3 IT will open ticket according to removal form, once completed, and signed off by IT official and ticket closed.

### 6.1.3 PASSWORD PROTECTION

Each employee is responsible for all the actions performed with his/her password, even if it's demonstrated that an action was carried out by another individual using the user's password. Users should therefore follow good security practices in the selection and use of passwords and keeping in mind:

6.1.3.1 Keep passwords confidential

6.1.3.2 Avoid keeping a record of passwords, e.g. hard copy or electronic file

6.1.3.3 Change passwords where there is any indication of possible system or password compromise

6.1.3.4 Avoid reuse or cycling of old passwords

6.1.3.5 Change passwords at regular intervals

6.1.3.6 Change temporary passwords at first logon

6.1.3.7 Never share individual passwords among users

### 6.1.4 UNATTENDED USER EQUIPMENT

All users should be made aware of the security requirements and procedures for protecting unattended equipment and implementation of such protection:

6.1.4.1 Terminate active sessions when finished, unless such sessions can be configured by an appropriate locking mechanism, e.g. a password screen saver.

6.1.4.2 Log computers off at end of session

6.1.4.3 Secure computers from unauthorized use by means of a key lock e.g. password access, when not in use.

### 6.1.5 CHANGE/MODIFICATION

Changes in user status include changes of job roles, responsibilities and transfers within the organization. Procedure as follows:

6.1.5.1 Change access form should be completed by user, signed by his/her supervisor and Head of Department.

6.1.5.2 Ticket will be opened according to change form and completed, signed off by IT official and ticket closed

### 6.1.6 REVIEW OF USER ACCESS RIGHTS

Review of user access rights is necessary to maintain effective control access to data and information services. Users access rights should be reviewed as follows:

6.1.6.1 Annually

6.1.6.2 After any changes such as promotion, demotion, termination.

6.1.6.3 Transfer from division to another within the same company.

### 6.1.7 PASSWORD RESET PROCEDURE

Procedure to verify the identity of a user prior to a password reset is the following:

6.1.7.1 Password reset form completed by user, his/ her Supervisor and Head of Department, form is send to IT Department.

6.1.7.2 Ticket opened for password reset, resented by IT Department.

6.1.7.3 Password is reset to default password of the system, user can change password at first logon. Passwords changed should conform to password standards.

6.1.7.4 IT Department closes ticket and sign off Password reset form.

### 6.1.8 PASSWORD REQUIREMENTS

The following password requirements will be set by the IT security department:

6.1.8.1 Minimum Length - 8 characters recommended

6.1.8.2 Maximum Length - 14 characters

6.1.8.3 Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:

- Lowercase
- Uppercase
- Numbers
- Special characters such as !@#$%^&*(){}[]

6.1.8.4 Passwords are case sensitive and the username or login ID is not case sensitive.

6.1.8.5 Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 12

6.1.8.6 Maximum password age - 30 days.

6.1.8.7 Account lockout threshold - 3 failed login attempts, the administrator reset the account lockout so they are aware of possible break in attempts on the network.

### 6.1.9 MONITORING OF USER ACCESS/ACTIVITIES

6.1.9.1 Access to log files, data files and databases are monitored and logs reviewed on regular basis by senior IT official.

6.1.9.2 Inactive users are monitored and must be blocked if inactive for 60 days.

6.1.9.3 Periodically checks are done once a quarter to remove or block redundant user accounts.

6.1.9.4 Repeated failed login attempts identified and investigated.

6.1.9.5 If an unauthorized intrusion is detected, it is reported to the IT Department.

6.1.9.6 System access logs are checked and signed by senior IT official, with date verified.

6.1.9.7 If any unusual activity is encountered it is entered into register and reported.

6.1.9.8 If internal unauthorized intrusion is detected on an account it is, disabled temporally, until formal reset procedure is done.

6.1.9.9 Where external intrusion is detected, all server, firewall, network and wireless device passwords should be changed immediately.

## 6.2 INFORMATION SECURITY AND STANDARDS

All involved systems and information are assets of the Municipality must be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

### 6.2.1 ANTIVIRUS/ANTI-SPYWARE

6.2.1.1 All servers and workstations MUST have an anti-virus and anti-spyware application installed that offers real-time scanning protection to files and applications running on the system.

6.2.1.2 Regular updates and scans of systems (servers) must be performed.

6.2.1.3 Although workstations can be monitored, scanned using Administrative console, users should ensure that workstations are updated and scanned weekly.

6.2.1.4 An exception to the above standards will generally be granted if the system is not a windows-based platform (ex. Linux, Unix)

6.2.1.5 Mail server must have an internal anti-virus scanning application that scans all mail destined to and from the mail server. Any system where non-technical or non-administrative users have access to the internet.

6.2.1.6 Any system where non-technical or non-administrative users have the ability to install software on their own.

### 6.2.2 GUIDELINES ON ANTIVIRUS/ANTI-SPYWARE

6.2.2.1 Delete spam, chain, and other junk email without forwarding it.

6.2.2.2 Never download files from unknown or suspicious sources.

6.2.2.3 Backup critical data and system configuration on a regular basis and store the data on the file server.

6.2.2.4 Always scan an external source device (external hard drive, USB stick, cd's, DVD's) for viruses before using it.

6.2.2.5 Never open any files or macro's attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your trash/deleted items.

### 6.2.3 ACCEPTABLE USE OF NETWORK INFRASTRUCTURE

6.2.3.1 Users must report any weaknesses in municipality's computer security, any incidents of possible misuse or violation to the appropriate management.

6.2.3.2 Users must not attempt to access any data or programs contained on the Municipality's system for which they do not have authorization or permission.

6.2.3.3 Users must not share their passwords, accounts, or personal identification numbers (pin) or devices used for identification and authorization purposes.

6.2.3.4 Users must not make unauthorized copies of copyrighted software.

6.2.3.5 Users must not purposely engage in activity that may threaten, degrade the performance of information resources.

6.2.3.6 Users must not run download, run or install security programs or utilities on the system, such as packet sniffers, password cracking programs or port scanners.

6.2.3.7 Users must not make excessive use of business resources.

6.2.3.8 Users must not intentionally access, create, store or transmit material which may deem to be offensive, indecent or obscene to the municipality.

### 6.2.4 INCIDENTAL USE

As a convenience to the user community, incidental use of Information Resources is permitted to the following restrictions:

6.2.4.1 Incidental personal use of email, internet access, fax machines, printers, and copiers and so on, is restricted to approved users; it does not extend to other acquaintances.

6.2.4.2 Use must not result in direct costs to the municipality.

6.2.4.3 Use must not interfere with the normal performance of an employee's work duties.

6.2.4.4 No files or documents may be sent or received that may cause legal action against, or embarrassment to the municipality.

6.2.4.5 Storage of personal email messages, files and documents must be nominal.

6.2.4.6 All messages, files and documents including personal messages, files and documents located on the municipality's Information systems are owned by the municipality, may be subject to open requests and may be accessed in accordance with this policy.

### 6.2.5 NETWORK ACCESS MONITORING

6.2.5.1 Users are permitted to use only those network addresses issued to them by IT Unit

6.2.5.2 All remote access (dial in services) to the municipality will be either through an approved connection or via an Internet Service Provider (ISP).

6.2.5.3 Remote users may connect to the municipality's Information Resources only through an ISP and using protocols approved by the municipality, but not financial system.

6.2.5.4 Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the network.

6.2.5.5 Users must not install network hardware or software that provides network services.

6.2.5.6 Non computer systems that require network connectivity must conform to the municipality's Information Technology Department policies standards.

6.2.5.7 Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. Users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the network infrastructure.

6.2.5.8 Users are not permitted to alter network hardware in any way.

6.2.5.9 Evidence of unauthorized access to privileged accounts will be monitored and reported to management.

6.2.5.10 The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency:

- Firewall logs
- User account logs
- Application error logs o System error logs
- Backup logs
- Help desk tickets

6.2.5.11 The following checks will be performed at least annually:

6.2.5.12 Password strength

6.2.5.13 Unauthorized network devices

6.2.5.14 Operating system and software licenses

### 6.2.6 SERVER SECURITY

Standards for the internal server equipment that is owned by the District Municipality, to minimize unauthorized access to information and manage operations, are as follows:

6.2.6.1 Configuration changes for production servers must follow the appropriate change management procedures.

6.2.6.2 Appropriate changes are made to business continuity plan.

6.2.6.3 Access to services should be logged and/or protected through access-control methods.

6.2.6.4 Services and applications that will not be used must be disabled where practical.

6.2.6.5 The most recent security patches must be installed on the system as soon as practical, the only exception being when it would interfere with business requirements.

6.2.6.6 Always use required password standard principles to access the systems to perform a function, exception being made to file server.

6.2.6.7 Ensure that telnet services are blocked.

6.2.6.8 SSH connection methods are preferred.

6.2.6.9 All windows firewalls must be active on servers if possible.

6.2.6.10 Do not use root when a non-privileged account will do.

6.2.6.11 Servers should be physically located in an access-controlled environment.

6.2.6.12 Servers are specifically prohibited from operating from uncontrolled area.

- The following information is required to identify server and operations: Server contact(s)
- Hardware and Operating System/Version
- Main Functions and applications
- Backup contact
- Yearly review of support contracts
- Licenses used

### 6.2.7 INTERNET ROUTER AND WIFI ROUTERS

All routers and switches connected to the District Municipality's production network must meet the configuration standards:

6.2.7.1 No local user accounts are configured on the router.

6.2.7.2 Password on the router must be enabled and must meet password standard principles.

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

6.2.7.4 Users must not attempt to disable or reconfigure the firewall software.

6.2.7.5 Encryption of at least 128-bit encryption must be used.

### 6.2.8 FIREWALL

The purpose is to establish and maintain control over the firewall rule sets.

6.2.8.1 Users must not attempt to disable or reconfigure the firewall software.

6.2.8.2 Password must meet password standard principles, changed on annually basis.

6.2.8.3 Deny all traffic (In both directions) which is not explicitly permitted in both directions (inbound and outbound)

6.2.8.4 Permit Inbound VPN access on network devices or servers.

6.2.8.5 IT Unit applies the Firewall Configuration Rules on the network to utilized as security device.

### 6.2.9 WIRELESS COMMUNICATION

This policy prohibits access to the Municipality's networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria have been granted an exclusive waiver by IT and are approved for connectivity to the network. This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the internal networks. This includes any form of wireless communication device capable of transmitting packet data.

Compliance

6.2.9.1 To comply with this policy, wireless implementations must: Maintain point to point hardware encryption of 256 bits. (WPA2-AES or WPA2-TKIP)

6.2.9.2 Maintain a hardware address that can be registered and tracked, i.e., a MAC address. Support strong user authentication (PSK)

6.2.9.3 Users must not attempt to disable or reconfigure the wireless communication software.

6.2.9.4 Password must meet password standard principles, changed on annually basis.

6.2.9.5 SSH and SSL connection methods must be enforced

6.2.9.6 Telnet ports disable.

6.2.9.7 Default name of administrator account must be changed.

### 6.2.10 ELECTRONIC STORAGE

Electronic Storage: All confidential information shall be stored on approved NAS (network attached storage) devices in a directory with no additional access and/or exposure beyond those with authorized business need.

6.2.10.1 Disposal/Destruction: The data should be removed when no longer needed to perform the functions of their job responsibilities.

6.2.10.2 Preferred method of connection should be SSL.

6.2.10.3 Password must meet password standard principles, changed on monthly basis.

### 6.2.11 SECURITY INCIDENTS REPORTING

6.2.11.1 Any security incidents experienced by a user experiencing password misuse, intrusion of systems etc. must be reported to Information Technology Department.

6.2.11.2 A Security incident form must be completed; to give detail description of incident occurred.

6.2.11.3 Users should attempt to stop any IT security incident as it occurs. Powering-down the computer or disconnecting it from the network will stop any potentially threatening activity.

6.2.11.4 IT Unit will troubleshoot incident and fixed actions will be noted.

6.2.11.5 IT Unit will make recommendations on how to improve, so that reoccurrence of same problem doesn't take place.

6.2.11.6 IT Unit must report all security incidents to the Director of Corporate services and Municipal Manager.

6.2.11.7 Where incident is related to a system or user account, that account will be locked or password will be immediately changed.

6.2.11.8 Logs relating to the security incidents are maintained.

## 6.3 ELECTRONIC MAIL STATEMENTS

### 6.3.1 WRITING EMAILS

Users shall adhere to the following rules when writing an e-mail:

6.3.1.1 Messages shall be professional and to the point.

6.3.1.2 The language used shall be presentable and convey the professional image of the municipality.

6.3.1.3 Spell checker shall be used before sending the message.

6.3.1.4 The signature shall be according to the municipality's standard with the disclaimer beneath the signature, i.e.

**AOBAKWE THUPAE**
**IT OFFICER**
**IT SECTION**
**CORPORATE SERVICES DEPARTMENT**

---

John Taolo Gaetsewe District Municipality

Phone: +27 (53)712 8700
Fax: +27 (53)712 2502



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

Local phone: 053 712 8756 / +27 (0)53 718700
Mobile:
email: thupaea@taologaetsewe.gov.za
WEB: http://www.taologaetsewe.gov.za

John Taolo Gaetsewe District Municipality
4 Federale Mynbou Street
P.O. Box 1480
8460

**Mr. KLAAS TEISE**
**MUNICIPAL MANAGER**

6.3.1.5 Attachments shall be compressed (zipped) where possible to reduce bandwidth usage.

6.3.1.6 Usage of the **cc:** and **bcc:** functionality shall be used only when required. The use of the **bcc:** function is not recommended.

6.3.1.7 Only important messages shall be marked as important,

6.3.1.8 Users shall only send, reply or forward any message to a maximum of five (15) persons at a time, unless prior approval is obtained from the relevant manager.

### 6.3.2 REPLYING TO AND EMAIL FORWARDING

Users shall adhere to the following rules when replying to and/or forwarding e-mails:

6.3.2.1 E-mails **received** shall be read within eight (8) working hours after receipt thereof.

6.3.2.2 **Replying** to an e-mail shall take place within eight (8) hours after receipt thereof.



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

6.3.2.3 E-mails flagged as a **high priority** shall be replied to within four (4) hours.

6.3.2.4 When a user shall be out of his/her office for more than twenty-four (24) hours, the Out of Office Assistant shall be enabled with an appropriate and professional message stating when the person shall be back in the office, as well as a contact person (with details) should the sender need an urgent reply on the mail. The Out of Office Assistant shall be disabled when back in the office.

6.3.2.5 When forwarding a message, the action that the recipient must take shall be stated.

### 6.3.3 PERSONAL EMAILS

Users shall adhere to the following rules for sending, receiving and forwarding personal e-mails.

6.3.3.1 Users shall not use the municipality's e-mail facility to send any graphics and/or non-work-related documentation.

6.3.3.2 Users shall not use the municipality's e-mail facility to send attachments with personal e-mails, ensuring adequate bandwidth for official e-mails.

6.3.3.3 Users shall not use the municipality's e-mail facility for personal e-mails that interfere with their work and performance.

6.3.3.4 Users shall not use the municipality's e-mail facility to forward any hoax messages, as those sometimes contain viruses.

6.3.3.5 Users shall not use the municipality's e-mail facility to forward any chain letters.

6.3.3.6 Users shall not subscribe to any newsletters or newsgroups without prior approval.

### 6.3.4 RESTRICTION ON MAILBOXES

6.3.4.1 Mailbox limits shall be set to 2GB per user, which shall restrain the user to send or receive e-mails as soon as the mailbox limit is exceeded.

6.3.4.2 Users shall be able to send and receive e-mail sizes of 5MB. If the size of the attachment or e-mail is larger than 5MB, the e-mail shall not be delivered.

6.3.4.3 Secretaries and Management shall have a mailbox size of 5GB and shall be able to send and receive e-mails less than or equal to 30MB.

6.3.4.4 In case of redirecting mailbox of one user to the other, both parties must be informed and written agreement signed.

### 6.3.5 MAILBOX MAINTENANCE

6.3.5.1 Users shall note that personal e-mail maintenance resides with the user and that the user shall delete any e-mail messages not needed to have a copy of.

### 6.3.6 MAILBOX RETENTION

6.3.6.1 E-mail accounts not used for 30 days shall be deactivated.

6.3.6.2 The Network Administrator shall not be held responsible for any mismanagement or loss of data in MS Outlook, since the user is the maintainer and owner of their own mailbox.

### 6.3.7 PROHIBITED CONTENT

The law requires e-mail users to strictly adhere to the following rules:

6.3.7.1 Users shall not use the e-mail system for the creation or distribution of any offensive, or disruptive messages, including messages containing offensive

comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability.

6.3.7.2 Users shall strictly not send or forward e-mails containing libelous, defamatory, offensive, racist or obscene remarks. The Municipal Manager shall promptly be notified if an e-mail of this nature is received.

6.3.7.3 Users shall not forward a message without acquiring permission from the sender first.

6.3.7.4 Users shall not send unsolicited e-mail messages.

6.3.7.5 Users shall not forge or attempt to forge e-mail messages.

6.3.7.6 Users shall not send e-mail messages using another person's e-mail account unless that person has authorized that.

6.3.7.7 Users shall not copy e-mail messages or attachments belonging to another user without the permission of the originator.

6.3.7.8 Users shall not disguise or attempt to disguise the identity of the sender of an e-mail message.

6.3.7.9 MailToAll must be requested from Municipal Manager Officer to be used.

6.3.7.10 IT Unit can use MailToAll to inform users about availability and non-availability IT related services

### 6.3.8 SENSETIVE INFORMATION

6.3.8.1 Users shall not use e-mail to discuss competitors, potential acquisitions or mergers or to give their opinion about another firm.

6.3.8.2 Users shall avoid sending confidential information by e-mail. If this has to be done, the information shall be secured by including it in a Microsoft Word or Excel file and protecting it with a password, and then the recipient is provided with the password by means of other communication, for instance by telephone.

6.3.8.3 All e-mail accounts maintained on the e-mail system are the property of the municipality.

6.3.8.4 Users shall not give passwords to other people.

### 6.3.9 ACTION TO BE TAKEN BY PERSONNEL

6.3.9.1 Users shall report the misuse of the e-mail facility to the IT department, who shall ensure that such complaints are dealt with in a professional, fair and quick manner.

6.3.9.2 Users shall not open an e-mail message when not sure who the sender of the e-mail message is.

### 6.3.10 MONITORING OF EMAILS

6.3.10.1 The municipality reserves the right to monitor e-mail messages to make sure the policy rules are being adhered to.

6.3.10.2 E-mail monitoring is very useful in a court of law, since it shows that the municipality is serious about preventing offensive messages and unlawful use of the e-mail facility.

6.3.10.3 Monitoring and filtering is essential to detect viruses and spam messages.

6.3.10.4 Monitoring and filtering of e-mails can save the municipality unnecessary loss of data.

### 6.3.11 THE USER`S ACCOUNTABILITY

6.3.11.1 A user's mailbox account may be restricted and abandoned immediately if in any case restrictions are not adhere to. The user shall then have to apply with his/her Manager as well as the IT Officer/Manager to reopen the e-mail account usage.

6.3.11.2 The municipality may institute disciplinary action against a user when found guilty of any e-mail misuse practices, which could result in legal action against such a user and/or suspension or dismissal.

6.3.11.3 All messages distributed, created, stored, sent or received on the municipality's e-mail system are the property of the municipality. Prior notice shall be given of the viewing of messages.

6.3.11.4 Acceptable use of e-mail is based on common sense, common decency, and civility applied to the electronic communications environment.

6.3.11.5 Users shall not use the municipality's e-mail system to send any non-work-related documentation and/or graphics.

6.3.11.6 Users shall, when out of the office for more than 24 hours, enable the Out-of-Office Assistant with an appropriate and professional message stating when the user shall be back in the office, as well as a contact person (with details), should the sender need an urgent reply on the mail; and again, disable the Out-of-Office Assistant when back in the office.

6.3.11.7 Users shall clearly state the action expected from the recipient when forwarding an e-mail message.

6.3.11.8 Users shall adhere to the Electronic Mail Usage Policy of the municipality. The approved policy shall be made available on the Intranet of the municipality.

## 6.4 INTERNET

### 6.4.1 INTERNET USAGE AND TOOLS

6.4.1.1 Software for browsing the Internet is provided to authorize users for business and research use only.

6.4.1.2 All software used to access the Internet must be part of the Municipal standard software suite or approved by the IT department. This software must incorporate all vendor provided security patches.

6.4.1.3 All files downloaded from the Internet must be scanned for viruses using the approved and current virus detection software.

6.4.1.4 All software used to access the Internet shall be configured to use the firewall.

6.4.1.5 All sites accessed must comply with the Acceptable Use Policies of the Municipality.

6.4.1.6 All user activity on the internet is subject to logging and review.

6.4.1.7 Content on all Municipal Web sites must comply with the Acceptable Use Policies of the Municipality.

6.4.1.8 No offensive or harassing material may be made available via Municipal Web sites.

6.4.1.9 No personal commercial advertising may be made available via Municipal Web sites.

6.4.1.10 Municipal internet access may not be used for personal gain or personal solicitations.

6.4.1.11 No Municipal data will be made available via Municipal Web sites without ensuring that the material is available to only authorised individuals or groups.

6.4.1.12 All sensitive Municipal material transmitted over external network must be encrypted.

6.4.1.13 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with Municipal records retention schedules.

### 6.4.2 ACCEPTABLE USE OF INTERNET

6.4.2.1 Incidental personal use of Internet access is restricted to Municipal approved users; it does not extend to family members or other acquaintances.

6.4.2.2 Incidental use must not result in direct costs to the Municipality.

6.4.2.3 Incidental use must not interfere with the normal performance of an employee's work duties.

6.4.2.4 Private use includes internet banking and newspaper websites only.

6.4.2.5 Using the internet to obtain business information for company use from commercial or academic web sites.

### 6.4.3 UNACCEPTABLE USE OF INTERNET

6.4.3.1 No files or documents may be sent or received that may cause legal liability for, or embarrassment to John Taolo Gaetsewe District Municipality.

6.4.3.2 Storage of personal files and documents within Municipal Information Resources should be nominal.

6.4.3.3 All files and documents – including personal files and documents – are owned by the Municipality, may be subject to open records requests, and may be accessed in accordance with this policy.

## 6.5 DESKTOP AND LAPTOP SECURITY

### 6.5.1 IT UNIT`S RESPONSIBILITY

6.5.1.1 The Information Technology unit shall be responsible for ensuring secure installations, configurations, distribution, management and removal from service, of John Taolo Gaetsewe District Municipality desktop and notebook computers.

6.5.1.2 The Information Technology unit must document if these responsibilities are delegated to any other party.

6.5.1.3 The Information Technology unit shall make available to users, a *list of authorized and accepted software and applications* approved by John Taolo Gaetsewe District Municipality.

6.5.1.4 Desktop and notebook computers shall be configured to reduce the risk of inadvertent or unauthorized access to John Taolo Gaetsewe District Municipality information and systems.

6.5.1.5 All John Taolo Gaetsewe District Municipality desktop and notebook computers shall be configured according to Information Technology unit's *Desktop and Notebook Configuration Standards.*

6.5.1.6 John Taolo Gaetsewe District Municipality standard virus detection software shall be installed on all desktop and notebook computers, mobile, and remote



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

devices and shall be configured to check files when read and routinely scan the system for viruses.

6.5.1.7 Server computers shall be configured to log all significant computer security relevant events. (E.g. password guessing, unauthorized access attempts or modifications to applications or systems software.)

### 6.5.2 ALL COMPUTER USERS OBLIGATION

6.5.2.1 Individuals granted access to the John Taolo Gaetsewe District Municipality Network or information systems shall secure desktop and notebook computers from inadvertent or unauthorized access.

6.5.2.2 When leaving a desktop or notebook computer unattended, users shall apply the "Lock Workstation" feature (ctrl/alt/delete, enter) where systems allow.

6.5.2.3 Desktop and notebook computer users shall not disable or alter security safeguards, such as virus detection software, installed on John Taolo Gaetsewe District Municipality desktop or notebook computers.

6.5.2.4 Physical security measures shall be used to secure notebooks, computer media, and other forms of information storage media containing confidential or sensitive information.

6.5.2.5 Notebook computers left in a vehicle shall not be visible. If possible, the notebook should be stored in a locked boot. (Weather conditions should be considered when leaving electronic equipment in a vehicle for long periods of time.)

6.5.2.6 Desktop computer users shall store confidential and sensitive information on a network drive (shared directory on the John Taolo Gaetsewe District Municipality Network) and the user's hard drive.

6.5.2.7 Notebook computers, computer media and any other forms of removable storage (e.g. diskettes, CD ROMs, zip disks, PDAs, flash drives) shall be stored in a secure location or locked cabinet when not in use.



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

6.5.2.8 Other information storage media containing confidential data such as paper, files, tapes, etc. shall be stored in a secure location or locked cabinet when not in use.

6.5.2.9 Peripheral equipment (e.g. printers, faxes, copiers) that store, produce and/or transfer confidential or sensitive information shall be protected from inadvertent or unauthorized access.

6.5.2.10 All documents containing confidential or sensitive information shall be cleared immediately from shared printers and copiers.

6.5.2.11 Individual users shall not install or download software applications and/or executable files to any John Taolo Gaetsewe District Municipality desktop or notebook computer without prior authorization from the Information Technology unit.

6.5.2.12 Desktop and notebook computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).

## 6.6 SERVER ROOM SECURITY

### 6.6.1 ALL COMPUTER USERS OBLIGATION

6.6.1.1 All internal servers deployed at John Taolo Gaetsewe District Municipality will be owned by the Information Technology unit which will also be responsible for system administration.

6.6.1.2 Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System version
- Main functions and applications, if applicable

6.6.1.3 Information in the corporate enterprise management system must be kept up-to-date.

6.6.1.4 Configuration changes for production servers must follow the appropriate change, management procedures.

6.6.1.5 Operating System configuration should be in accordance with approved Information Technology standards.

6.6.1.6 Services and applications that will not be used must be disabled where practical.

6.6.1.7 Access to services should be logged and/or protected through access-control methods, if possible.

6.6.1.8 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

6.6.1.9 The standard security principles of *"least required access"* to perform a function will be applicable to all systems and user accounts.

6.6.1.10 Servers must be physically located in an access-controlled environment.

6.6.1.11 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

6.6.1.12 All security-related events on critical or sensitive systems must be logged and audit trails saved and kept online for a minimum of 1 week.

6.6.1.13 Server security-related events must be reported to the IT Specialist who will review logs and report incidents to management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific
- applications on the host

## 6.7 PATCH MANAGEMENT

### 6.7.1 TECHNIQUE

6.7.1.1 Workstations and servers owned by JTGDM must have up-to-date (as defined by ITU's minimum baseline standards) operating system security patches installed to protect the information assets from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by JTGDM.

### 6.7.2 WORKSTATION

6.7.2.1 Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by JTGDM. Any exception to the policy must be documented and forwarded to the ITU for review.

### 6.7.3 SERVERS

6.7.3.1 Servers must comply with the minimum baseline requirements that have been approved by ITU. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the ITU information assets and the data that resides on the systems. Any exception to the policy must be documented and forwarded to ITU for review.

## 6.8 DATA BACKUP AND RESTORATION

### 6.8.1 MEDIA RETENTION

6.8.1.1 Application servers' daily backups will be retained for a period of one month.

6.8.1.2 Application servers' month-end backups will be retained for a period of twelve months.

6.8.1.3 Application servers' year-end backups will be retained for three (3) years.

### 6.8.2 RESTORATION OF BACKED-UP FILES

6.8.2.1 All requests for file recoveries should be made by completing and submitting the file recovery request form – form DR1 to the IT Manager

### 6.8.3 ARCHIVING OF FILES

6.8.3.1 Files will be archived immediately after the IT department has been notified that a user has officially separated with the John Taolo Gaetsewe District Municipality according to the rules laid down in the User Account Policy.

### 6.8.4 OFFSITE STORAGE ON NAS DEVICE

6.8.4.1 A duplicate of backup material shall be stored at an off-site location. Sufficient software and instructions must be made available at the off-site storage location to ascertain full restoration of the backups should the need arise.

6.8.4.2 The NAS device will be located at Tourism office or Technical Services workshop

### 6.8.5 DATA TO BE BACKED-UP

6.8.5.1 User data stored on the server hard drive.

6.8.5.2 System state data

6.8.5.3 The registry Systems to be backed up include but are not limited to:

- File server
- Mail server

## 6.9 INFORMATION TECHNOLOGY STRATEGIC PLANNING

### 6.9.1 MAIN COMPONENTS

6.9.1.1 Information systems

6.9.1.2 Information technology

6.9.1.3 Information management

### 6.9.2 PROCESS

6.9.2.1 The person responsible for IT within the John Taolo Gaetsewe District Municipality will be responsible for the development of the IT Strategic Plan

6.9.2.2 The IT Steering Committee will review the plan on a quarterly basis to ensure it remains current and support the business objectives.

6.9.2.3 The IT Strategic Plan will form the foundation for the annual capital budget.

## 6.10 PHYSICAL PROTECTION OF IT ASSETS

### 6.10.1 PRIORITIES

6.10.1.1 The most important protection measures are listed below reflecting the relevant rating of importance of each. The municipality will implement the measures in the order of importance starting with the measures rated as "high"

| Security Measure | Importance |
|---|---|
| Raised floor | Medium |
| Air conditioning system | High |
| Uninterrupted Power Supply | High |
| Fire protection system | Medium |
| Access control system | High |
| Security camera's | Low |

| | |
|---|---|
| Monitoring alarms | Medium |

6.10.2 **RAISED FLOOR**: An anti-static raised floor system that will ensure ease of reticulation within the room as well as accommodating the air conditioning / ventilation to the server cabinets.

6.10.3 **AIR CONDITIONING SYSTEM**: A good air conditioning system in a computer room is vital to ensure the availability of computer systems as well as extending the life of the equipment.

6.10.4 **UNINTERRUPTED POWER SUPPLY**: The UPS system will improve availability of the computer systems as well as protect data by eliminating the abnormal shut down of the servers.

6.10.5 **FIRE PROTECTION**: The fire protection system should not only detect fires but should automatically release gas to suppress the fire.

6.10.6 **ACCESS CONTROL SYSTEM**: One of the most effective access control systems consists of magnetic door controllers operating via a digital key-pad reader system/finger scan with release buttons on the inside of the room.

6.10.7 **SECURITY CAMERA**: Security cameras can assist in identifying the cause of intentional damage.

6.10.8 **MONITORING ALARMS**: A GSM based system to warn the support staff in the case of any alarm condition within the computer room will form a vital component of the safe guarding of IT equipment or data. The GSM-operation ensures that the warning device is not dependant on any of the internal factors such as power, LAN, etc. in order to generate the relevant alarm. The following conditions can be monitored:

- **Flood.** This means that there is water present under the access floor, which poses a threat to the electrical and networking reticulation.
- **Fire alarm**. Early warning in the case of a fire or if gas is about to be discharged into the room.
- **Temperature.** By installing multiple temperature sensors in the server room it will be possible to send an alarm if the temperature exceeds a pre-determined limit.
- **UPS power.** Four alarms can be obtained directly from the UPS: These are:
- Mains power failure,
- Bypass active,
- Common alarm (a generic alarm which indicates that the UPS needs maintenance for any one of several reasons) and a

## 6.11 IT STEERING COMMITTEE

### 6.11.1 MEETING INTERVALS

6.11.1.1 Bi-annually.

### 6.11.2 MEMBERS OF THE STEERING COMMITTEE

6.11.2.1 Municipal manager
6.11.2.2 Senior IT Officer
6.11.2.3 Heads of Department, or a delegate nominated by HOD, provided that the delegate is given the mandate to represent the HOD at this forum

## 6.12 IT STEERING COMMITTEE TERMS OF REFERENCE

**John Taolo Gaetsewe DM – ICT Steering Committee Terms of Reference**

### 6.12.1 BACKGROUND

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

6.12.1.1 The role of the ICT Steering Committee ("the Committee) has evolved over time. Many organisations face the challenges of making the ICT a value add-activity and strategic business enabler, moreover sustaining value, effectiveness and interest throughout the organisation and through the alternating cycles of ICT and business strategic planning and implementation.

6.12.1.2 The vital role of ICT can no longer be ignored by the municipality and it have become critical that the municipality focus on ICT governance.

6.12.1.3 The role of the Committee is not to focus on 'steering' a single department/division, but concentrate on the Information and Communication Management function that permeates the entire organisation.

6.12.1.4 In September 2009, the revised King Code and Report on governance ("KING III"), was released. King III sets out a number of key governance principles under which ICT should conform and the principles must be seen against the legislative requirements contained in the 2008 Act and the Public Finance Management Act of 1999. This is reflected in the terminology used in King III with "must" indicating a legal requirement and "should" indicating where application of King III will result in good governance.

6.12.1.5 Apart from the KING III, it is now also a requirement of the Auditor General that an ICT Steering Committee exists within organisations and should therefore be acknowledged by Management/Council as the governing body for ICT within the organisation.

6.12.1.6 SA Apart from the KING II and Auditor General, organisational ICT should adhere to various other legislations. This includes inter alia the:

- ECA 2002 (Electronic Communications Act)
- ECSA 2002 (Electronic Communications & Security Act)
- ICASA (Independent Communications Authority of South Africa)
- ITA (Information Technology Agency) responsible for I.T Code of Ethics through all sectors of ICT
- SALRC – South Africa Law Reform Commission – Email & Internet

Laws, etc.

- TELECOMMUNICATIONS ACT (TCA 1996)
- Department of Communications Regulatory
- Other ACTs with reference to ICT, such as MFMA, CPA2009, ECTA2002, etc.

6.12.1.7 It should now be apparent that the need for an ICT governing body is not just a legal requirement, but it is a necessity within the municipality

### 6.12.2 PURPOSE AND FUNCTION

6.12.2.1 The purpose of this is to establish an ICT Steering Committee to govern and be accountable for the municipality's ICT environment and ensure that ICT conforms to legislation.

6.12.2.2 The Committee will advise, in terms of an oversight role, to Management/Council on all matters relating to ICT and be responsible for:

- The investigating, considering and steering of high level/impact ICT projects.
- The prioritizing of proposed high level projects.
- The constant reviewing of approved projects.
- Facilitating the achievement of optimal ICT management.
- Enhancing the understanding and satisfaction with the value of ICT investments.
- Encouraging constituent ownership of ICT projects and endorsement of ICT policies.
- Fusing the ICT and business strategies, goals, and resources, and achieving competitive advantage through ICT.
- Encouraging a collaborative work environment and fosters trust via mutual credibility and responsiveness.
- The revision of the draft ICT budget and budget processes.
- Mediating conflicts in priorities and/or departmental perspectives that may not be in the best interest of the municipality.

### 6.12.3 COMPOSITION AND TERM OF OFFICE OF THE COMMITTEE

6.12.3.1 The Committee must comprise the following:

- The Chairperson
- One representative from each directorate of which a deputy Chairperson should be elected.
- One representative from the procurement office
- Specialist where applicable, example, a representative from the asset management division

6.12.3.2 The term of office for the Committee members will be concurrent with the Municipal Financial year. Each term therefore comprises 12 months and will be served as follows:

- The Chairperson and Deputy Chairperson will serve for one (1) term where after an election process should be conducted.
- Members will serve a two consecutive terms where after Departmental directors can nominate new representatives.

6.12.3.3 The Municipal Manager must appoint the Committee members through a formal appointment letter that clearly indicate the term of membership

### 6.12.4 ICT RESPONSIBILITY

6.12.4.1 An I.T official will attend all meetings and will only be functional as follow:

- Where applicable, present projects to the Committee.
- Assist the Committee in clarification of ICT matters.
- Provide the necessary technical support.

6.12.4.2 The ICT division will remain responsible for the ICT operational requirements of the municipality, overseen by the Committee.

6.12.4.3 Quarterly reports will be presented to the Committee for approval and acceptance to ensure good governance.

### 6.12.5 MEETINGS

6.12.5.1 For a committee meeting quorum to be achieved, a minimum of four (4) members must be present.

6.12.5.2 Minutes must be taken of all meeting, preferably by Secretariat division, and distributed electronically to all members within fourteen (14) days.

6.12.5.3 At least four meetings should be scheduled per term, unless otherwise decided by the Committee.

6.12.5.4 Agendas should be sent to all members at least five (5) days prior to the scheduled meeting.

6.12.5.5 Agenda items should be sent to the Chairperson, or nominated member, at least seven (7) days prior to the scheduled meeting.

6.12.5.6 Items for discussion at a scheduled meeting that is not on the agenda will only be sustained at the discretion of the Chairperson.

6.12.5.7 All corrections to minutes must be tabled at the scheduled meeting, before confirmation

### 6.12.6 VALIDITY

6.12.6.1 The Terms of Reference as set out herein and approved by Management/Council will be valid for a period of one (1) year, where after it must be reviewed and presented to Management/Council for approval.

### 6.12.7 ACTIVITIES OF THE COMMITTEE

6.12.7.1 The Committee must keep proper records.

6.12.7.2 Review the internal and external Service Level Agreements of ICT.

6.12.7.3 Formally note and accept the manner in which it will function.

6.12.7.4 Prepare an official Code of Conduct that will be included with the appointment letters of all members.

### 6.12.8 ACCOUNTABILITY

6.12.8.1 The Committee will be held accountable for ICT governance and to make binding decisions in terms of the municipality's ICT requirements. Regular reports should be presented to Management/Council regarding the developments of ICT in the organization

## 6.13 IT CHANGE MANAGEMENT

**6.13.1** Every change to John Taolo Gaetsewe DM Information resources such as: operating systems, computing hardware, networks and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

**6.13.2** All changes affecting computing environmental facilities (e.g. air-conditioning, water, heat, plumbing, electricity, networking and alarms) need to be reported to or coordinated with the leader of the change management process.

**6.13.3** A formal written change request must be submitted for all changes, both scheduled and unscheduled.

**6.13.4** All scheduled change requests must be submitted in accordance with change management procedures so that the Head of Information Technology has time to review the request, determine and review potential failures and make the decision to allow or delay the request.

**6.13.5** Each scheduled change request must receive formal Change Management approval before proceeding with the change.

**6.13.6** The Head Information Technology may deny scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backup plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays or during special events.

**6.13.7** Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.

**6.13.8** A Change Review must be completed for each change, whether scheduled or unscheduled and whether successful or not.

**6.13.9** A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

- Date of submission and date of change
- Owner and custodian contact information
- Nature of the change
- Indication of success or failure

**6.13.10** All John Taolo Gaetsewe DM information systems must comply with an Information Resources change management process that meets the standards outlined above

## 6.14 IT CHANGE MANAGEMENT PROCEDURE

All critical changes and/or updates will be applied using the following procedures. Optional changes and or updates will be applied only as an on needed basis to correct problems.

### 6.14.1 INITIATING A CHANGE

6.14.1.1 Only the IT teams have access to the request for change form to initiate emergency changes.

6.14.1.2 All other requests for changes either from users and anywhere else in the organisation need to be considered as to how they can be initiated, i.e. via the service desk.

6.14.1.3 It is the responsibility of the Change Initiator to ensure that a sufficient detail exists in the request for change to ensure that the IT Manager can make an informed assessment.

6.14.1.4 Change information should include the following:

- *The reason/business justification for the change*
- *Why the change is needed – in particular giving detailed information on implications of not implementing the change – i.e. security risks etc.*
- *Known risks or impact to the business of implementing the change – consideration should also be given to the risk and impact to the business of not implementing the change*
- *Required resources – i.e. people*

### 6.14.2 ASSESSMENT

6.14.2.1 Filtering and assessing a change

- All changes (except those that can be dealt with via a standard change or a change model for which operational procedures exist) are filtered and assessed by the IT Manager.

6.14.2.2 Rejection of changes at assessment stage

- Where a request for change has been assessed and considered inappropriate, impractical or unjustified they should be returned to the Initiator, together with brief details of the reason for the rejection, and the request for change should record the rejection information.
- A right of appeal against rejection should exist, via normal management channels.
- The status of a change rejected at this stage of the change process will be: REJECTED BY THE IT MANAGER

6.14.2.3 Progression of changes at assessment stage

- If the IT Manager completed the change assessment and considers it request viable the request for change is progress to prioritisation. The status of a change at this stage of the change process will be: ASSESSED.

### 6.14.3 AUTHORISATION OF A CHANGE BY THE IT MANAGER

- If the request for change has a priority of any level other than significant or major importance, the IT Manager has the authority to authorise and delay such changes.
- The status of a change at this stage of the change process will be: AUTHORISED.

### 6.14.4 RISK ASSESSMENT AND TESTING

- ITU will assess the effect of a change on the JTGDM infrastructure prior to its deployment. ITU will also assess the affected change for criticality relevant to each platform (for example, servers, desktops, laptops, etc.).
- If ITU categorizes a change as an Emergency, ITU considers it an immediate threat to the JTGDM network. Therefore, JTGDM assumes greater risk by not implementing the change, than waiting to test it before implementing.
- Changes deemed critical or non-critical will undergo phased implementation for each affected platform before release for implementation. IT Services will expedite testing for all critical changes, where applicable.

### 6.14.5 NOTIFICATION AND SCHEDULING

- ITU Management must approve the schedule prior to implementation. Regardless of criticality, each change release requires the creation and approval of a 'Request for Change' (RFC) prior to implementing the change.
- The ITU Management Group will decide when notifying staff is necessary.

## 6.15 IT ASSETS REPLACEMENT

### 6.15.1 IT EQUIPMENT REPLACEMENT PROCEDURE

6.15.1.1 IT Equipment replacements within the municipality will be identified by the use of a device life cycle, coupled with the source of funding.

6.15.1.2 The equipment specifications will be reviewed (led by ITU) on a six monthly basis (more frequently if necessary) with formal approval by the ITSC.

The table below illustrate the recommended replacement periods and method of IT Equipment

| Equipment | Replacement/Upgrading/License renewal Period | Replacement Method |
|---|---|---|
| Workstation | 3 years | Purchase or Lease |
| Laptop | 3 years | Purchase or Lease |
| Tablet | 3 Years | Purchase or Lease |
| Software | 1 year | Lease or Purchase |
| Printer | 5 years | Purchase or Lease |
| Switch | 2 years | Purchase |
| Radio Link | 3 years | Purchase |
| 3G/Modem | 2 years | Lease |
| Storage Device | 4 years | Purchase or Lease |
| Server | 4 years | Purchase or Lease |
| WAN/LAN | 5 years | Purchase or Lease |

### 6.15.2 TAILORED IT EQUIPMENT

6.15.2.1 On certain occasions like for like replacements are not appropriate or fit for purpose so instead tailored hardware is required.

6.15.2.2 Each department has equal opportunity to request tailored IT hardware which differs from the agreed standard specification.

6.15.2.3 Any such request must however be supported by clear rationale as to why the standard entry level alternative would not meet the business need and why the proposed IT hardware needs to be at the specified level.

6.15.2.4 All requests for tailored IT hardware or software must be presented to the ITSC for approval before being put forward for investment consideration. To ensure continuity and facilitate informed decision making, only requests which are presented using the attached pro-forma will be considered by the ITSC.

6.15.2.5 The ITSC has a duty to fully consider each business case for tailored hardware, assessing the criteria already identified on the pro-forma when making a judgment on any specialist requirements. All requests which are turned down by the group should be accompanied by advice on alternative measures or solutions.

### 6.15.3 DISPOSAL OF OBSOLETE IT EQUIPMENT

Items can be available for disposal because they are:

6.15.3.1 Not capable of running required operational software/being upgraded.

6.15.3.2 Reached the life cycle.

6.15.3.3 No longer required, due to changed procedures, functions or usage patterns.

6.15.3.4 No longer complying with occupational health and safety standards.

6.15.3.5 Beyond repair but able to be sold for scrap or being donated for cause.

### 6.15.4 OPTIONS FOR DISPOSAL OF IT EQUIPMENT

Equipment identified for disposal may be dispensed with using the procedures below. Acceptable methods of disposal are: -

6.15.4.1 Transfer of the equipment to project under municipal funding or the related.

6.15.4.2 Private Sale.

6.15.4.3 Donated to a community service organisation subject to the provisions of Municipality`s Asset Management Policy.

6.15.4.4 Destroyed or recycled

6.15.4.5 Choice of the most appropriate disposal option will normally be influenced by the age and functionality of the equipment for disposal and by market value.

6.15.4.6 In all cases assets disposed of must be reported to ensure they are removed from the central Inventory.

A more detailed description of each disposal option is set out below.

| Disposal Option | Description |
|---|---|
| Sale | Private sale involves assigning a price to the item(s) and publicizing the item(s) availability for sale and setting a closing date for receipt of bids. This may range from a newspaper advertisement to a general Email notice and in some instances sealed bids. To ensure a fair price is paid in the case of a private sale, a market value assessment should be obtained, in writing, from the Finance Director. Prospective buyers should be given adequate opportunity to inspect the goods prior to sale. Collection or forwarding of the goods is normally contingent on the presentation to Budget and Treasury Department of evidence of payment of the sale price. The item may, on receipt of an offer, be sold to the first person to make such an offer. |
| Donation | The Municipality may authorize the donation of the equipment to another organisation. Ideally, such donations should be to organizations and not to individuals. The preferred recipient of such donations by the Municipality should be partnership |

| | |
|---|---|
| | primaries. All donations must be approved by municipal council. |
| Destroyed or Recycled | Items with no market value and no use to any other organisation or person may be destroyed in an appropriate and safe manner. ITU will identify IT equipment for disposal and recommend disposal method of which an 'Asset Disposal' form must be completed and authorized by the Finance Director and forwarded to Assets Management Unit for updating of the Asset Register. |

## 7. Roles and Responsibilities

7.1 **Windows Administrators** will manage the patching needs for the Microsoft Windows servers on the network.

7.2 **Workstation Administrators** will manage the patching needs of all workstations on the network.

7.3 **Firewall/Antivirus System Administrators** will manage the updating and patching needs of all workstations and servers installed with the antivirus system on the network.

7.4 **IT Officer:** will be responsible for approving the major and emergency patch management deployment requests, requested through Change Request procedures.

- Approved server configuration guides must be established and maintained by the Information Technology unit and for each server in the live production environment
- Establish a process for changing the configuration guides.

7.5 **User:** to ensure that, at the time of a system reboot, all jobs-in-progress and unsaved changes are saved to prevent possible data loss.

7.6 Overall responsibility for the IT equipment register is shared between the **Finance Director, Asset Management Unit** and **ITU,** who will make any, decisions related to accounting for and disposing of assets subject to approval by the council.

7.7 **ITU:** will manage this policy and update it appropriately in consultation with the ITSC.

7.8 **ITU**: will submit 3 year budget following appropriate discussions/consultation with the ITSC.

7.9 **The Municipal Manager**: is the custodian of data backup and restoration policy and will through the IT unit enforce compliance to the requirements of this policy. Any exceptions to comply with this policy must be approved by the custodian

7.10 **IT Technician**

7.10.1 Will execute the day to day tasks and activities necessary to ensure that a backup is conducted and successfully completed.

7.10.2 Will upon discovery immediately report any problems that are preventing or may prevent the successful execution and completion of the backup process.

7.10.3 Will make available upon request, copies of reports of any specific backup jobs.

7.10.4 Will ensure the proper labeling, changing and replacing of media and safe storage on and offsite of all used backup media.

7.10.5 Will within ten minutes, make available upon request, any specific backup tape or set of tapes. Tapes that have been stored offsite must be made available within 48 hours of the initial request.

7.10.6 Will conduct data restore after the restore process has been approved by the IT Security Specialist.

7.11 **Executive Secretary to the Municipal Manager:** Shall be the custodian of spare keys to the server room. Shall record the name and designation of each person accessing the key and including the purpose and date on each it was used.

7.12 **Information Owner:** Data and records stored on Municipal systems are presumed to be the property of the Municipality. For purposes of this Policy, the "owner" of a collection of information will be the Municipal employee responsible for the creation of that information or the primary user of that information. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual. Owners have the responsibility to:

7.12.1 Know the information for which they are responsible.

7.12.2 Determine a data retention period for their information, in accordance with the municipality records retention schedule (and any applicable state or federal laws or regulations).

7.12.3 Ensure appropriate procedures are in effect to protect the integrity, confidentiality, and security of the information used or created within their area.

7.12.4 Authorize access and assign custodianship.

7.12.5 Specify controls and communicate the control requirements to the custodian and users of the information.

7.12.6 Report promptly to the Information Security Officer the loss or misuse of Municipal information.

7.12.7 Initiate appropriate actions when problems are identified.

7.12.8 Promote education and awareness by utilizing programs administered by the Information Security Officer, where appropriate.

7.12.9 Follow existing approval processes within their respective organizations for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

7.13 **Custodian:** The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

7.13.1 Providing and/or recommending physical safeguards.

7.13.2 Providing and/or recommending procedural safeguards.

7.13.3 Administering access to information.

7.13.4 Evaluating the cost effectiveness of controls.

7.13.5 Coordinating the maintenance of information security policies, procedures and standards as appropriate and in consultation with the Information Security Officer.

7.13.6 Promoting education and awareness by utilizing programs administered by the Information Security Officer, where appropriate.

7.13.7 Report promptly to the Information Security Officer the loss or misuse of Municipal information.

7.13.8 Initiate appropriate actions when problems are identified.

7.14 **User:** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

7.14.1 Access information only in support of authorized job responsibilities or role within the Municipality.

7.14.2 Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

7.14.3 Refer all disclosures of confidential information to the relevant manager.

7.14.4 Keep authentication devices (e.g. passwords, Secure-cards, PIN's, etc.) confidential.

7.14.5 Report promptly to the Information Security Officer the loss or misuse of any authentication device.

7.14.6 Report promptly to the Information Security Officer the loss or misuse of Municipal information.

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

7.14.7 Initiate appropriate actions when problems are identified.

7.15 **User Management Role:** Municipal staff who supervise users as defined above or who handle unit administrative responsibilities or as designated by head unit. User management is responsible for overseeing their user's access to information, including:

7.15.1 Reviewing and approving all requests for access authorizations.

7.15.2 Initiating security change requests to keep security record current so they accurately reflect the users role and required access.

7.15.3 Promptly informing the appropriate Information Security Officer of employee terminations and transfers.

7.15.4 Revoking physical access to terminated employees, i.e., confiscates keys, change combination locks, etc.

7.15.5 Revoking physical access to students and others when access to information is no longer needed or appropriate.

7.15.6 Providing the opportunity for training needed to properly use the computer systems.

7.15.7 Reporting promptly to the Information Security Officer the loss or misuse of Municipal information.

7.15.8 Initiating appropriate actions when problems are identified.

7.15.9 Follow existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

7.16 **Information Security Officer Role:** The Municipal Information Security Officer is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Municipal Manager. Specific responsibilities include:

7.16.1 Ensuring security policies, procedures, and standards are in place and adhered to.

7.16.2 Providing basic security support for all systems and users.

7.16.3 Advising owners in the identification and classification of computer resources.

7.16.4 Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.

7.16.5 Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.

7.16.6 Providing on-going security education.

7.16.7 Performing security audits for compliance.

7.16.8 Responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

7.16.9 Shall ensure that physical access to any server equipment is controlled.

7.16.10 Review and approve all production server configuration changes.

7.16.11 Will ensure that the backup policy is updated as necessary with changes that may occur in the environment

7.16.12 Will ensure that the requisite software, hardware, on and offsite media storage locations and consumables are available to ensure compliance with this policy.

7.16.13 Will be responsible for the periodic assessment of compliance with this policy and to take any corrective measures where necessary.

7.16.14 Will be responsible for determining from time to time critical data whose backup related costs are financially justifiable.

7.16.15 Will ensure that an up to date list of folders that form part of the backup sets is available in both electronic format and hardcopy.

7.16.16 Will be responsible for authorizing any data restores that may be necessary.

7.17 Prior to submitting a request for tailored IT equipment, ITSC representatives must exercise due diligence and be convinced that the request satisfies the principles of this policy.

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

7.18 When reviewing requests for tailored IT equipment all ITSC representatives should be prepared to challenge any requests which do not appear to comply with the principles of this policy.

## 8. IMPLEMENTATION AND MONITORING

8.1 Information Security and Internal Audit may conduct random assessments to ensure compliance with the policy without notice.

8.2 Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the JTGDM issue tracking system and support teams shall be dispatched to remediate the issue.

8.3 Repeated failures to follow policy may lead to disciplinary action.

8.4 ITU will manage the hardware IT equipment register with the assistance of the Asset Management Unit.

8.5 It is essential that any moves or transfer of IT equipment are provided to ITU and Asset Management Unit to ensure the register is kept up to date.

8.6 All users are expected to read their E-mail regularly – at least twice per day (first thing in the morning, and at lunch-time.).

8.7 No users should send unnecessary messages ("please get ABC to contact me now") to large groups of people within the Municipality.

8.8 No users should forward e-mail from outside that is "spam" – i.e. chain-letters, request for help with worthy causes, etc

8.9 With due regard to the South African Constitution and the regulation of interception of the Communications Act and Provision of Communications Related Information Act, in order for the municipality to effectively manage its electronic communication resources the municipality reserves the right to intercept, monitor, block, delete, read and act upon any incoming or outgoing e-mail message addressed to or originating from the employee.

8.10 The Municipality reserves the right to grant or revoke the right to access of any equipment either issued for off-site usage or to be used on the premises in the event of misconduct from any employee

8.11 Implementation of this policy is in line with procedural diagrams and forms in Annex "A"

## 9. ENFORCEMENT

9.1 Implementation and enforcement of this policy is ultimately the responsibility of System Administrators together with the Users. Deployment of such services may be enforced through the system policies and Push Technology systems.

9.2 Implementation and enforcement of this policy is ultimately the responsibility of all departments with involvement of ITU and Asset Management Unit under the leadership of Finance Director and Corporate Services Director.

9.3 Microsoft Windows Server Update Services (WSUS) will be used to deploy the latest Microsoft product updates to computers running Microsoft windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows® XP, Microsoft windows 7 and Microsoft windows 8 operating systems.

MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

9.4 By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

9.5 Network Administrator must manage and distribute updates through the WSUS Administration Console, which can be installed and accessed on any Windows computer in the work domain.

## 10. EXCEPTIONS

10.1 Exceptions to the patch management policy require formal documented approval from ITU.

10.2 Servers, laptops and desktops and the related machines that do not comply with policy must have an approved exception on file with ITU.

## 11. REFERENCE

11.1 Assets management policy.

## 12. DISCIPLINARY ACTIONS

Violation of this policy may result in disciplinary action, which may include termination for employees; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subjected to loss of JTGDM Information Resources access privileges, civil and criminal prosecution.

## 13. ANNEXURES

**A - Network Access Request Form**
**B - Application to Change Password Form**

# Network Access Request Form

**PERSONAL INFORMATION**

Date _____

Name (Last, first, middle initial) _____ Employee Number _____

Street address _____ City _____ ZIP Code _____

Job Title _____ phone number _____ E-mail address _____

**Systems Request**

☐ Print/Copy/Scan (LAN Printers) ☐ Internet ☐ Sage 300 People

☐ Sage-Accounting ☐ TeamMate(Audit) ☐ E-Mails

**Acknowledgement Statement**

I _____ have read and understand the corporate information policies and I agree to adhere to the stated requirements. I also understand the signing of this page does not constitute a contract, nor is it to be construed as such; rather, my signature only indicates I have read the enclosed policies and will comply with same.

Name: _____

Signature: _____

Date: _____

**Approved by Head of Department : Manager/Director**

Name _____ Surname _____

Department _____

Signature _____ Date _____

**IT Use Only:**

**ACCOUNT CREATED BY :** _____ **IT equipment Asset#** _____

Date: _____ Signature _____



MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

# Application to change password

TO ENSURE THE SECURITY OF YOUR ACCOUNT, WE REQUIRE POSITIVE PROOF OF IDENTIFICATION FROM YOU, BEFORE WE CAN PROCESS YOUR REQUEST.

**Surname:** **First Name:**

**Username or Account:** **E-mail Address:**

☐ **Password to Change:** ☐ **Windows** ☐ **Sage Evolution** **sage 300 People**

**(Specify Below for Other System)**

**Telephone Extension:** **Department:**

**Unit :**

**Please note:**

**We will reset your password to "1234@taolo". The change will take effect within an hour of our receiving this request. Our operating hours are: 07:30 to 4:30, Monday to Friday. Any forms received outside of these hours, will only be processed the next day. Alternatively, send your form to IT Department.**

**Password security:**

**After we have received the form, wait 20 minutes and then restart computer and change your password from "1234@taolo" to a new password of your choice. This is for compliance with JTGDM Information Technology Policy**

**Acknowledgement Statement by User:**

**I have read and understood JTGDM Information Technology policies and I agree to adhere to the stated requirements. I also understand the signing of this page does not constitute a contract, nor is it to be construed as such; rather, my signature only indicates I have read the enclosed policies and will comply with same.**

- **I hereby authorize IT Security Officer to make the changes I have requested above.**
- **I also acknowledge that, for security reasons, I am responsible for changing my password once it has been reset to "1234@taolo" by your IT Unit.**
- **I agree that IT Unit and cannot be held responsible for any unauthorized access to any service provided by IT Unit Personnel.**

Name: _____

Signature: _____

Date _____

| TO BE COMPLETED BY THE IT UNIT PERSONNEL | | |
|---|---|---|
| I _____ performed the request above of resetting password for the above mentioned user as specified. | Signature: | Date: |



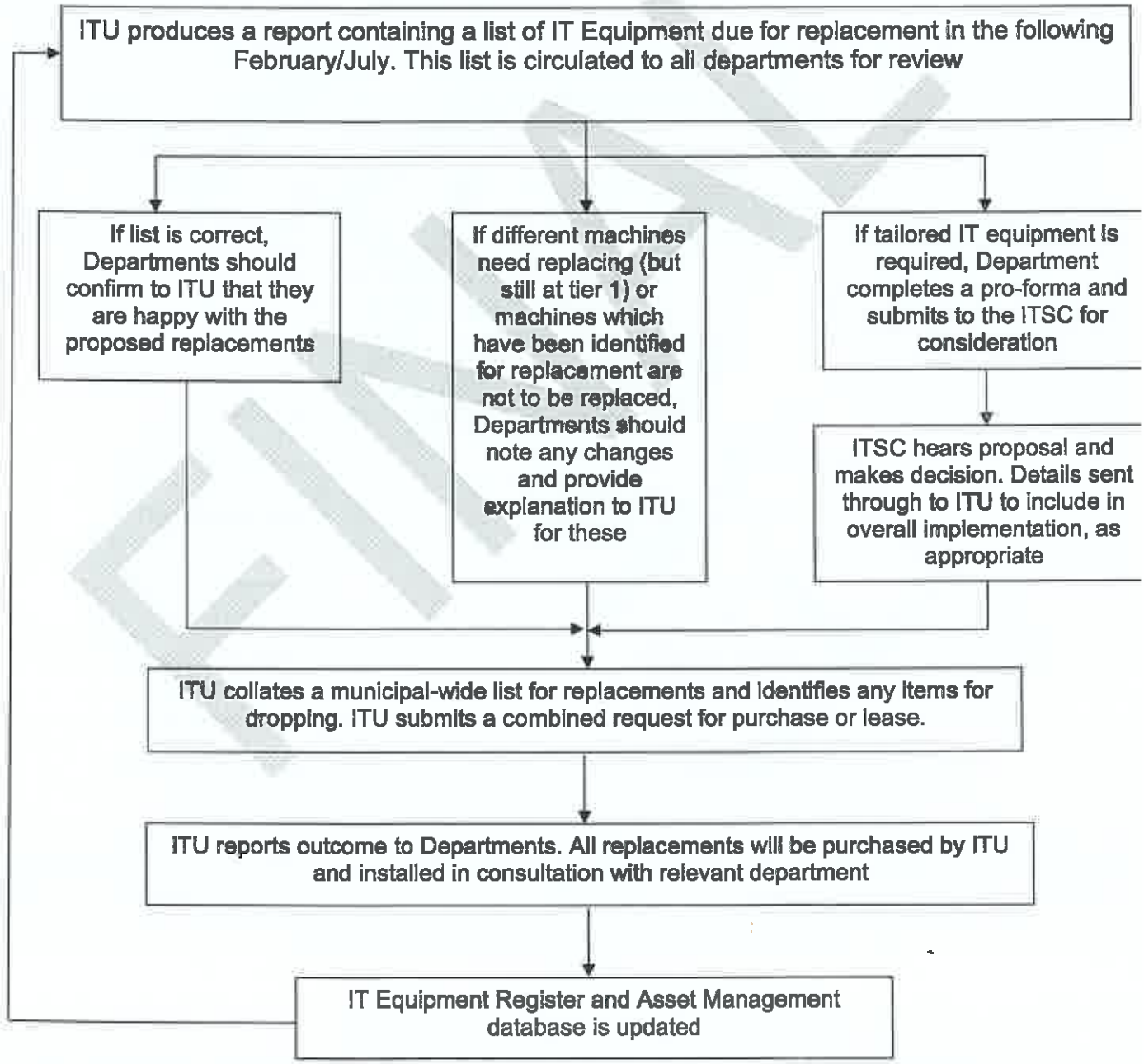
MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

# Procedural Diagrams and Forms on IT Equipment Replacement/Disposal

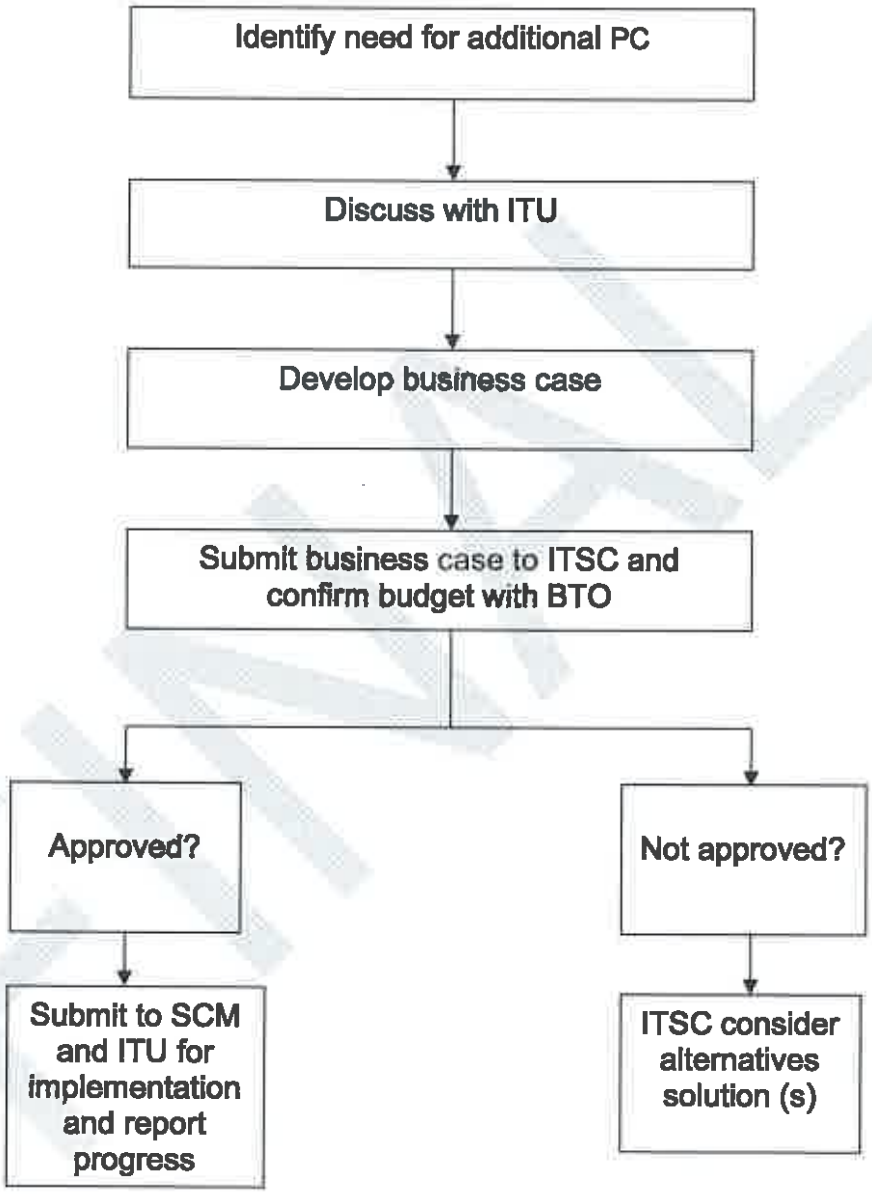
## Annex "B"

### IT EQUIPMENT REPLACEMENT PROCESS

**Note:** Investment for all IT Equipment replacements will be requested by ITU twice a year in April and November. Lists for replacements will be sent to departments in February and July to allow time to review and submit any changes



## REQUESTING AN ADDITIONAL EQUIPMENT (LAPTOP, PC OR PRINTER ETC.)






MR. I.E AISENG
JOHN TAOLO GAETSEWE
DISTRICT MUNICIPALITY
SPEAKER

## PRO-FORMA FOR TAILOR MADE IT EQUIPMENT REPLACEMENT

Pro -forma requests should be completed for each individual business case (e.g. for each specific staff user or for each specific project). All business cases must be inclusive of VAT and should append any supporting information (e.g. resource allocation for project usage) as appropriate.

**Request Summary**

| | |
|---|---|
| Proposed by | |
| Department | |
| Actual differential (or additional) cost of bespoke machines (replacement cost of bespoke PCs – replacement cost of standard PCs) | |
| Summary of bespoke requirement | |
| Business implications of not approving | |

**Equipment Details**

| | |
|---|---|
| Variations to standard machine specification (attach supporting spec detail if necessary) | |
| Rationale for non-standard replacement | |
| Type of equipment (PC, Mac, notebook etc.) | |
| No of machines requested | |
| User/Staff | |
| Any additional peripherals (e.g. docking station) | |
| Image (generic or specialist) | |
| | |

**Estimated Costs**

| | |
|---|---|
| Quote attached? | |
| Estimated investment amount (including VAT) | |
| Anticipated replacement cycle | |
| Maintenance issues | |
| Any displacement opportunities or redundant machines? | |
| Specification of existing equipment (to be displaced/replaced) | |
| Any interrelated or concomitant costs? (e.g. software upgrades) | |

**Location Details**

| | |
|---|---|
| Location | |
| Accessibility of machine location (e.g. sole user, shared during office hours, 24/7) | |
| Space rationalization opportunities (hot desking/sharing) | |
| Space integration opportunities (can the equipment be integrated with other spaces and have dual purpose) | |
| Typical machine usage (e.g. pay slip printer or cheque printer) | |

**Other supporting comments for consideration**

| |
|---|
| |