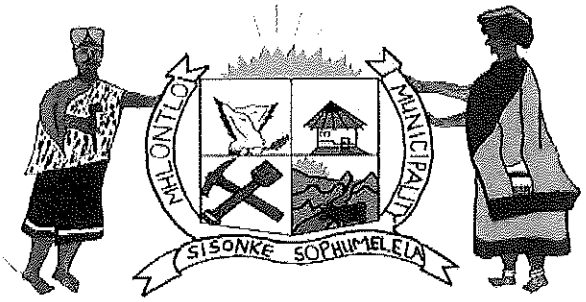

MHLONTLO LOCAL MUNICIPALITY ICT GENERAL CONTROL FRAMEWORK

Financial Year: 2019 - 2020

MHLONTLO LOCAL MUNICIPALITY

Purpose

To provide a high level control framework for the embedment of IT General controls within the environment of Mhlontlo Local Municipality

Scope of Framework

Information Technology Planning
Acquisition and implementation
Information Technology Delivery & Support
Information Technology Security
Disaster Recovery

Policies and Procedures

Applicable policies and procedures relating IT General Control processes.

Legislative

Applicable legislation and standards including: Municipal Finance Management Act(MFMA), Minimum information Security Standards(MISS) and Treasury Regulations, Municipal Laws and regulations.

Control Objectives per Process

1. IT Strategy, Budget and Policy

The IT strategy is developed and understood, and budgets are aligned

2. ICT Steering Committee

ICT Steering Committee governs the ICT function

3. ICT Risk Assessment

ICT Risks are assessed on an ongoing basis

4. Third party management

All IT service providers are identified, managed and monitored in accordance with service level agreements

5. Change management

All changes to the IT systems (including hardware, networks and software) are managed to minimise the likelihood of disruption, unauthorised alterations and errors

6. IT project management

Risks related to IT projects, are minimised and managed in order to identify and control events that may lead to project delays and budget overruns.

7. IT acquisition management

The organisation follows a formally documented policy/procedure for the acquisition of new IT equipment / systems.

8. Monitoring of IT performance

Performance and capacity of IT system is adequately managed in order to minimise potential disruption

9. Skills programs

System users are adequately trained to ensure effective use of the IT systems.

10. Incident management
Incidents are reported, resolved, monitored and escalates appropriately

11. Protection of IT equipment
Computer facilities are appropriately protected against environmental hazards

12. User access management
Type and level of user access are authorised, appropriately assigned and protected in order minimise unauthorised access

13. Network security management
Security of the network perimeter is appropriately monitored and managed

14. Virus and Patch management
To ensure IT environment is adequately protected from viruses/spyware

15. Audit logs
Periodic review of the system activities/events are undertaken in order to reduce the risk of errors, fraud, misuse or unauthorised alteration

16. Business continuity management
Effective measures are in place to minimize business impact in the event of a disaster

Processes 1: IT strategy, budget and policy

Control objective: The IT strategy is developed and understood, and budgets are aligned

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) An IT strategy has been defined and is aligned to the municipality's strategy, and is updated at least once in two years. This may include the following: -Objectives -ICT Vision -Goals -Challenges -Section and Services -Governance -ICT Strategy -Revision of ICT Strategy -Time Frames -Commencement of ICT Strategy	General Manager: Corporate Services(GM-CS)	ICT Manager	once in two years	IT Strategy
b) The IT budget is defined and actual vs. budget is monitored by the GM-CS on a regular basis.	GM-CS	ICT Manager	Annually	IT budget Review of actual spend vs. budget
c) An appropriate individual is assigned the responsibility for IT security	Municipal Manager(MM)	GMCS	Annually	Letter for the assignment of the roles and responsibilities

				of the Information Security Officer. Roles and Responsibilities of person made responsible for Information Security
d) IT Policies are developed which governs the IT environment. These may include: - Overall ICT policy (Integrated ICT Policy) - User access management policy - Change management - DRP policy	MM	GMCS	Annually	IT Policies

Process 2: ICT Steering Committee

Control Objective: ICT Steering Committee governs the ICT functions

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
An ICT Steering Committee exists and meets according to the requirements of the ICT Governance Policy, to discuss the progress ICT makes in terms of its strategy	GMCS	GMCS	Quarterly	Charter/terms of reference Minutes of meeting

Process 3: ICT Risk Assessment

Control Objective: ICT risk are assessed on an on-going basis

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
A comprehensive annual ICT risk assessment is performed, with updates throughout the year to ensure it remains current for the year.	GMCS	ICT Manager	Annually	ICT Risk Register

Process 4: Third Party Management

Control Objective: IT service providers are identified, managed and monitored in accordance with service level agreements.

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Contracts exist to formalise all key relationships with current IT service providers for IT hardware and software maintenance, networks, telephony, etc. These contracts should include the following: **-Minimum required service levels** **- Key performance indicators (KPIs) Requirements for monthly performance reporting from service provider** **- Penalties for contact violation or non-performance.**	MM	GMCS	on - going	Contract for each IT service provider. Contracts with clearly defined SLA.
b) Management regularly reviews performance of service providers against KPIs and against agreed minimum service levels	- GMCS	- ICT Manager	- On – Going	Minutes of action taken or escalation where required

Process 5: Change Management

Control Objective: All changes to the IT systems (including hardware, networks and software) are managed to minimise the likelihood of disruption, unauthorised alterations and errors

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Define and implement a change management process that covers the following at application level, database level and operating system level for each of the key applications: - business justification and approval - nature and priority of changes - changes are assessed for impact - back out plan exists - changes are tested before being moved into production environment where applicable - level of approval and sign-off required before moving change into production environment - If service provider access is required, the access provided is temporary and follows the user access request process.	ICT Unit	ICT Manager	On - going	Change management procedure. Change log. Change request forms (including evidence of testing).
b) Management reviews compliance to change management process on a monthly basis.	GMCS	ICT Manager	Monthly	Monthly review of changes

Process 6: ICT Project Management

Control Objective: Risks related to ICT projects, are minimised and managed in order to identify and control events that may lead to project delays and budget overruns

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
A general project management framework is defined. This may include: - the scope and boundaries - the allocation of responsibilities - task breakdown - budgeting of time and resources - milestones or check points - approvals	GMCS	ICT Manager	ADHOC	ICT Integrated policy

Process 7: IT Acquisition Management

Control Objective: The organisation follows a formally documented policy/procedure for the acquisition of new IT equipment / systems

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
A formally documented policy/procedure is defined and followed for the acquisition / procurement of new IT equipment / systems. This is included in the overall Municipal procurement policy.	GMCS	ICT Manager	ADHOC	Integrated ICT Policy

Process 8: Monitoring of System Performance

Control Objective: Performance and capacity of IT system is adequately managed in order minimise potential disruption

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a)The performance and capacity management standards exist to minimise potential disruption.	GMCS	ICT manager	Monthly	Performance and Capacity management standards
b)Performance and capacity, for example disk space, memory etc. of IT systems is appropriately planned and regularly monitored by management.	ICT Unit	ICT Manager	Monthly	Review of performance and capacity logs

Process 9: Skills Programs

Control Objective: System users are adequately trained to ensure effective use of the IT systems

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
Establish effective education programs of all users of IT systems, this includes: - identifying the training needs of each user group - providing training to each user group as needed	GMCS	ICT Manager/HR Manager	ADHOC On – going	Confirmation of IT staff training & Informal on the job training on the use of IT services New users induction/training form

Process 10: Incident Management

Control Objective: Incidents and service requests are reported, resolved, monitored and escalates appropriately

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Incidents (for example users cannot log on, system not available, network is down, or hardware) and service requests are logged on a Microsoft Excel Spread sheet. The incidents are prioritised and the ICT Unit instructs the service provider immediately on issues requiring resolution. The ICT Unit maintains the log sheet.	ICT Unit	ICT Manager	Daily	Integrated ICT Policy ICT Fault Register
b)The log sheet is reviewed on a monthly basis to ensure that the incidents have been recorded accurately, prioritised and resolved in a timely manner.	ICT Unit	ICT Manager	Monthly	Review of ICT Fault Register
c)Long outstanding incidents have been appropriately escalated.	GMCS	ICT Manager	On – going	List of long outstanding incidents and escalation

Process 11: Protection of IT Equipment (Computer Facilities)

Control Objective: Computer facilities are appropriately protected against environmental hazards

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Physical access to computer facilities in the municipality is restricted to authorised individuals. E.g. Where IT equipment is in a separate room, this must be secured by a lock and key, visitors access register should be kept and signed. Management review this register	ICT Manager	ICT Officer	On – going	Physical security of IT equipment (e.g. Access keypad) Server Room Access register
b) Relevant environmental control standards are defined and should include the following: - Fire suppressant devices such as hand held extinguishers available at the entry point to the room. - Smoke detectors. - UPS is installed and secured inside the server room.	ICT Manager	ICT Officer	On – going	Protection of IT equipment policy Fire suppressant devices Smoke detectors

- UPS is tested on an annual basis. - IT equipment/connections raised above the floor level - Air conditioners or temperature controlled cabinet, where server room is not present.				Air conditioners/ temperature controlled cabinet Equipment/connections raised above floor UPS Testing of UPS

Process 12: User Access Management

Control Objective: Type and level of user access are authorised, appropriately assigned and protected in order minimise unauthorised access

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Overall IT security policy, end user security policy, Email/internet use age policy and user access management policy is defined. Password parameters are included in the end user/ overall IT security policy which include the following: - Minimum length - Complexity - Expiry period - History - Forced change on initial logon - Number of failed login attempts before account lockout - Lockout duration	GMCS	ICT Manager	On going	Overall IT security policy End user security policy (containing password parameter standards) Email/internet usage policy Password parameter settings
b) User accounts are well controlled, which includes: (i) User accounts are only created and maintained based on documented and approved requests which are retained (as part of the audit trail). (ii) Inactive users and/or leavers are locked/removed on a timely basis, (iii) Users are uniquely identified on the system through their user IDs, which follow a standard naming convention, (iv) System accounts, Default accounts, have had the passwords changed or are otherwise appropriately restricted. (v) Review of user access to ensure access rights support the segregation of incompatible functions.	ICT Manager	ICT Officer	On going -Reviews Quarterly	User access management procedure List of users created and corresponding user access request forms Quarterly review of user access rights
c) File system permissions are set appropriately, i.e. access to administration tools and system utilities are restricted to authorised personnel.	ICT Manager	ICT Officer	On going	File permissions

Process 13: ICT Security Management

Control Objective: Security of the ICT environment is appropriately monitored and managed

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Establish a plan to monitor and manage connections such as: - Connection to public networks and - Remote connections. - Third party connections	GMCS	ICT Manager	-Ongoing	ICT Integrated Policy
b) Adequate firewalls/ alternative security protection, e.g. gateway, are in place to protect against denial of services and any unauthorised access to the internal resources. Adequate security placed on routers, e.g. using software such as Terminal Access Controller Access-Control System (Tacacs +)	ICT Manager	ICT Officer	Ongoing	Approved firewall rule set/alternative security protection
c) Configuration standards exist for systems that support key services. Management periodically review and evidence compliance with each: - Operating system configuration standard (Windows, UNIX, OS/400, OS); and - Database configuration standard (Oracle, DB2, MS SQL).	ICT Manager	ICT Officer	Annually	Approved configuration standards Risk Acceptance or waiver form

Process 14: Virus and patch management

Control Objective: The IT environment is adequately protected from viruses/spyware

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Antivirus software is installed on servers, workstations and laptops. This antivirus software should be regularly updated. Antivirus log files should be reviewed on a regular basis.	ICT Manager	ICT Officer	Monthly	ICT Integrated Policy Up to date antivirus software Review of antivirus logs
b) Processes for deployment of security patches are defined and implemented. This includes frequency of patch management, systems/applications in scope, testing of patches and reviews to ensure patches have been deployed.	ICT Manager	ICT Officer	Monthly	ICT Integrated Policy

Process 15: Audit Logs

Control Objective: Periodic review of the system activities/events are undertaken in order to reduce the risk of errors, fraud, misuse or unauthorised alteration

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
Logs for the application, database, operating system are maintained and reviewed, these include: - User creation, modification and deletion (including dormant accounts) - Profile/role creation, modification and deletion - System and security parameter modification	ICT Manager	ICT Officer	Monthly	Audit log review procedure Activation of Audit Logs Review of Audit Logs

Processes 16: Business Continuity Management

Control objective: Effective measures are in place to minimize business impact in the event of a disaster

Key Financial Controls	Process owner	Control owner	Frequency	Evidence
a) Establish and document the backup process that will include the following: - Backup frequency, - Process to follow in the event of backup failures, - Offsite storage of backups, - Retention period of backups.	ICT Manager	ICT Officer	Daily	Backup and restoration management procedures Evidence of successful backups Offsite storage Escalation of backup failures Testing of backups

Policy Approval

This Policy was approved at a full Council Meeting held on 31 day of MAY (Month) 2019 (Year) at MHLONTLO Municipality.

Name and Surname	Designation	Signature
Nomfumeleko Dyudi	Mayor	
SOTSHONGAYE, SG	MM	