Molemole Municipality

ICT Policies and Procedures

ICT Procedure Manual

Document Name: **ICT Procedure Manual**

Document Information

Section	Policy Management
Policy	Policy Framework
Applicability	This document provides the basis for all policies, procedures and standards within the scope of the ICT Policy Framework.
Situations	This document is a general document outlining the framework and is applicable to all situations in which policies, procedures and standards are applicable within the scope of the ICT Policy Framework.
Change Log	V001 : Initial Version

Contents

Executive Overview: One-Page Introduction

This document provides a general framework for Policy Management and Administration that has been adapted for use in municipalities.

A Policy Framework includes the complete scope of activities for the implementation and enforcement of policies including:

- **Roles**: the people who will manage the policies and the roles that they play
- **Processes**: the processes which the Roles will engage in and
- **Policies**: the specific policies which are required to be managed including their associated Procedures, Forms, Standards and Practice Notes.

The purpose of this Policy Framework is to provide an environment in which policies can be created and managed, to ensure the policies can be an effective and efficient instrument to protect the information and ICT resources of the municipality. This protection is a fundamental requirement of each municipality in terms of the MFMA and the MSA based upon the fact that municipal information and ICT resources fall within the scope of the assets and resources identified in the relevant Acts.

This Policy Framework has been developed on the basis that the policies are under a management regime of continuous improvement – implying that there are always better ways to use policies effectively to achieve the ends of proper resource management and information security and to identify and control improper usage as early as possible.

The Policy Process Cycle is implemented in three phases which are called Approving Policies, Implementing Policies and Changing Policies.

Through the implementation of policies it is possible to ensure the proper utilisation of the municipality's expensive and essential ICT infrastructure and to ensure effective protection of municipal information.

Introduction to the Policy Framework

Founding Premises

The ICT Policy Framework is premised on the following:

- Information is a critical asset of the municipality.
- The ICT infrastructure which stores, processes and secures this information is a critical resource of the municipality.
- Both Information and the ICT Resources fall within the scope of municipal assets that are required to be handled in terms of the Municipal Finance Management Act (MFMA), and as a result, the municipality has a fundamental and non-negotiable responsibility to protect this information and the ICT resources which manage this information.
- The implementation of ICT Policies is an effective way to comply with the legal requirements of the MFMA and other legislation.
- The ICT Policies and their associated procedures and standards are required to comply with all relevant legislation and good practices.
- The key responsibility for asset management lies with the accounting officer, and in the case of information technologies this responsibility is delegated to the IS Manager.
- Misuse of information and information technologies is a basic violation of the terms of employment for municipal employees.
- The introduction of a set of ICT Policies, Procedures, Standards and Forms is one way to protect information but this needs to be supported by other controls for a complete solution to control objectives for ICT. Other controls will include an effective management structure, an ethical culture, as well as a practical and workable approach to penalties for violation.
- Everyone who has any form of contact with municipal information via ICT (information and communication technologies) of the municipality must be bound by the policy framework.

- Policies and procedures and their associated standards, guidelines and forms must be communicated effectively to all stakeholders.
- All policies are subject to continual review and improvement and the policy management processes must accommodate this.

What Comprises the Policy Framework

The Policy Framework consists of a set of related Roles and Processes which collectively support the effective management of the individual Policies, Procedures and Standards.

Roles

This includes all Roles within the scope of Policy Management, including those who make policies, those who approve policies, those who enforce policies, those who are subject to policies, those who review policies, as well as those who penalise violations of policies. Collectively, these Roles make up the organisational structure of the Policy Framework.

Processes

A comprehensive set of Processes need to support effective implementation of the policies. Within the Policy Framework these processes are structured into three separate groups.

Policies

Each Policy deals with situations that occur in the usage and management of information and ICT services and they dictate how to deal with these situations.

Each Policy identifies (1) all relevant Procedures, which formalise the actions to be taken within the Policy, (2) any Standards, which dictate required specifications to adhere to when implementing the Policy, which may themselves be a reference to international practice and (3) Forms, which are used for application and controls for situations in which signed approval is required to ensure compliance. Where necessary (4) Practice Notes are also included to support the realities of the implementation environment.

Glossary of Terms

This glossary contains words and terms that have special meaning in the context of the Policy Framework.

This starts with the definitions of the core terms of Policy, Procedure, Guideline and Standard, and then provides a tabular structure for more specific terms.

Each individual Policy document provides definitions of terms that are specific to the policy.

Definitions of Core Terms

There are many definitions for the key terms of Policy, Procedure, Guideline and Standard and we have taken the elements from a number of published definitions to arrive at one suitable for this ICT Policy Framework.

Policy

Definition

A Policy describes the required behaviour that a given person is required to comply with in a given situation together with the penalties for violating this required behaviour.

The key elements of this definition are:

- Situation: the situation or context with which the person is presented and in which they can take action.
- Person: this is generally intended to mean a single individual. However this could also mean group responsibility.
- Behaviour: this is intended to mean a set of actions which are required to be performed.
- Penalty: this is the outcome if the behaviour is not complied with.

Reference Sources

www.sans.org

"A formal, brief, and high-level statement or plan that embraces an organisation's general belief, goals, objectives, and acceptable procedures for a specific subject area.

Policy attributes include the following:

Require compliance (mandatory)

Failure to comply results in disciplinary action

Focus on desired results, not on means of implementation

Further defined by standards and guidelines."[1]

Microsoft Operations Framework

A policy explains what to do in a particular set of circumstances by providing necessary rules and requirements and by setting expectations about conduct. Policies help organisations clarify performance requirements, communicate management's intent for how work should be done, and establish accountability and the foundation for compliance."2

Example

Consider the Email Policy, in which the usage of the email facilities needs to be controlled with specific behaviours.

- SITUATION: The receipt or sending of email messages through the municipal email system.
- PERSON: All users of the email system.
- BEHAVIOUR: Usage of Email for municipal purposes only. Special handling of attachments to minimise virus infestation. No large attachments. No personal email. No junk email. No jokes through email. No distribution lists beyond reasonable sizes. No proliferation of email that is not directly related to work. Responsibility to report violations by others.
- PENALTIES: Minor offences (counselling on first offence, followed by verbal warning, written warning, final written warning, termination). Major offences (written warning as first offence, followed by other). Criminal offences (handled through police on first offence). Refer to the HR discipline code for dealing with offenders.

[1] A Short Primer for Developing Security Policies. Michele D. Gaul, The SANS Institute, 2007.

[2] Microsoft Operations Framework 4.0. Policy Service Management Function. P2.

Procedure

A Procedure is a series of steps which form a process. These, together with associated information, tools and components, enable the behaviour described in a Policy to be carried out in practice.

A procedure should be a fixed process without ambiguity.

Each Procedure has the following elements:

- STEPS: To be carried out in sequence, with different pathways through the steps as required.
- ROLES: People who are required to carry out each step, for situations in which there is more than one.
- EXCEPTIONS: Situations in which the procedure may fail and how this should be dealt with.
- FORMS/REGISTERS/RECORDS: Various records which may need to be captured at various points in the procedures.

In some cases the procedures may be simple and it is not necessary to document each of the steps and other elements.

Reference Sources

Microsoft Operations Framework

"Procedures break policies down into detailed steps that describe how work should be done and identify who should do what."[3]

Standard

A standard (or benchmark) is a behaviour which is deemed to be acceptable or required in a given context.

Standards are generally given in the form of specifications which must be adopted as the measure of acceptable behaviour, and in particular to distinguish between acceptable and unacceptable behaviours.

For example, consider the UserID and Password Policy, which includes statements on how to authenticate new users to the systems and networks, including the strength of the passwords which are considered to be acceptable. This Policy will make use of a Standard on Password Strength, which may require that all passwords contain at least 6 characters and at least 2 other characters, that the password has a maximum lifetime of 30 days, and a new password cannot be the same

[3] Microsoft Operations Framework 4.0. Policy Service Management Function. P2.

as the past 10 passwords used by this same user. This is a Standard, since it is a specification of what constitutes an acceptable password, rather than how this will be used in practice, which is contained within the Policy and the Procedure.

Guideline

A Guideline is a set of sample behaviours which will guide the implementation of a Policy or the execution of a Procedure in cases in which Standards are not available or in which there is a need for more specific examples.

Guidelines should bring the reader in touch with real-world situations and where possible should provide exemplars to illustrate how to behave in sample situations.

Term	Definition
Assigned Role	These are Roles specific to the IT Policy Framework.
(the) Committee	In most cases refers to the ICT Policy Committee.
Configuration Manager	This is a delegated responsibility of the ICT Policy Committee that is responsible for keeping the "original" copies of the policies and all related documents, in both physical and electronic form. They are also responsible for the distribution and control of the policies.
Council	The Council of the Municipality.
Guidelines	See Definition of Core Terms above.
ICT Policy	A Policy as identified in the context of this Policy Framework.
ICT Policy Committee	This is an internal committee consisting of specific individuals (Chairman, Policy Manager) as well as key managers within the IT Department and other SBUs who will provide the inputs to direct the Policy Framework and its implementation.
ICT Policy Framework	The complete set of ICT Policies required for the IS Department, together with the Processes to manage the Policies and the Roles who participate in the Processes.
ICT Policy Manager	The ICT Policy Manager is a single individual who is given the primary responsibility for the management, administration and oversight of all of the ICT Policies. Their specific responsibility is to ensure smooth implementation of the Policies, Procedures, and Forms.
IS Manager	The Manager of the IS SBU.
Local Labour Forum	The Local Labour Forum represents the constituency of users within the scope of municipal employees.

Term	Definition
Mayoral Committee	The Mayoral Committee will take the primary responsibility in recommending Policies for approval by the Council. To carry out their work they will liaise with the Local Labour Forum.
Named Role	A type of Role within the ICT Policy Framework consisting of existing committees and forums who play a part in the Policy Processes and for whom working with the ICT Policies is a part of their responsibilities.
Policy	See Definition of Core Terms above.
Policy Approvers	They are responsible to ensure that the policies as written and edited meet the requirements of the municipality, and that they represent the views and aspirations of all stakeholder communities, in particular the Council, Management and Employees of the municipality. Visitors and the Community are included to the extent that they are impacted by the policies.
Policy Auditors	They are required to verify the compliance to the ICT Policy Framework through various assurance practices and processes. They perform both an auditing role as well as a consulting role.
Policy Committee	The same as ICT Policy Committee
Policy Communication	This role is responsible for the effective communication of the policies. To formulate the communication strategies to ensure that all employees have access to the policies through various means, including newsletters, the intranet, posters, seminars and workshops.
Policy Educators	This Role has the function of training the Policy Enforcers about a Policy in terms of how to apply the Policy. As required, this Role may also involve general training of selected employees on specific policies, as well as developing training materials and running train-the-trainer courses. The Policy Educators will help to establish policy awareness within employee orientation programmes and related workshops. It is assumed that the basic employee training will be conducted by existing training personnel and performed as part of orientation and re-orientation training programmes.
Policy Enforcers	Policy Enforcers are those who are responsible for ensuring that specific policies are enforced properly. There could be one specified Policy Enforcer for each individual policy.
Policy Issue	This is a document received from any stakeholder indicating feedback or comments on any individual policy or the policy framework as a whole. This is the only way in which changes can be made to the Policy Framework and this provides the trigger that commences a change.

Term	Definition
Policy Issues Log	A Log of all Project Issues indicating relevant information such as who raised the issue and when, what is the substance of the issue, what type of issue it is, and how this was decided on.
Policy Implementer	The implementation of policies includes the establishment of the processes for enforcement. This will include the establishment of the total environment for the enforcement.
Policy Owner	Each Policy Owner is required to keep track of the implementation and enforcement of the Policy during the Implementation Process and to report back on the following questions.
Policy Reviewers	Policy Reviewers will evaluate the effectiveness of the policies to ensure that they are delivering the benefits as expected. They will monitor the policy implementation in terms of the violations and penalties.
Policy Writers/Editors	Policy Writers are individuals who write the policies using the inputs from the organisation as well as from external sources such as legislation, national policies and international best practices. Policy Editors will turn the created policies into documents which are easy to read and clearly understood by those who are required to abide by them.
Practice Notes	Same as Guidelines.
Procedure	See Definition of Core Terms above.
Role	A Role is a set of responsibilities as identified within the ICT Policy Framework. Each Role is assigned to one or more persons, organisational units. See : Named Roles, Assigned Roles
SBU	Strategic Business Unit – the primary business units of the municipality
Stakeholders	The set of Stakeholders in terms of the Policy Framework includes all Roles as identified including those who make policies, those who approve policies, those who enforce policies, those who are subject to policies, those who review policies, as well as those who penalise violations of policies. Collectively, these Roles make up the organisational structure of the Policy Framework.
Standard	See Definition of Core Terms above.

Process Summary

The ICT Policy Framework outlines a number of processes which are used in the management and administration of the Framework.

This section provides an initial summary of these for ease of reference for those who are required to implement these processes.

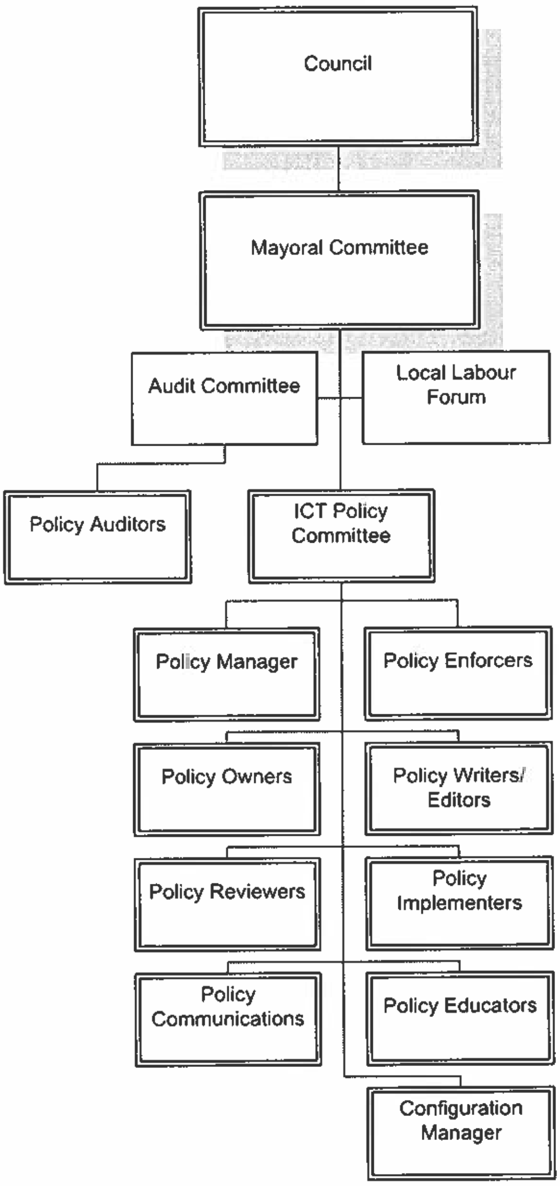
This provides the basis on which the Policy Framework becomes a living document.

Process	Responsibility	Description	When
Committee Processes			
	IS Manager	Produce the Constitution of the ICT Policy Committee and submit this for Approval by the Mayoral Committee	Once-off
	Mayoral Committee	Approve the Constitution of the ICT Policy Committee	Once-off
	IS Manager	Update the composition of the ICT Policy Committee	As required
	IS Manager	Schedule and conduct meetings of the ICT Policy Committee	Monthly
	IS Manager	Appoint the ICT Policy Manager	As required
Risk Management			
	ICT Policy Manager	Risk Identification	As noted
	ICT Policy Manager	Risk Analysis	Monthly
(AP) Approving Policies			
AP-1	Policy Writer	Writing Policies	
AP-2	Policy Editor	Editing Policies	
AP-3	ICT Policy Committee Policy Reviewers	Validating Policies	

Process	Responsibility	Description	When
AP-4	Mayoral Committee ICT Policy Committee	Approving Policies	
(IP) Implementing Policies			
IP-1	Policy Communications	Communicating the Policies	Continuous
IP-2	Policy Educators	Training on the Policies	Ongoing
IP-3	Policy Owner ICT Policy Committee	Implementing the Policies	Continuous
IP-4	Policy Enforcer HR SBU	Enforcing the Policies	On violation
IP-5	Policy Owner ICT Policy Committee	Monitoring and Reviewing the Policies	
IP-6	Internal Audit SBU	Auditing the Policy Framework and Policies	Regular
IP-7	Risk Owners ICT Policy Manager	Risk Management (see above section for details of Risk Identification and Risk Management processes)	
(CP) Changing Policies			
CP-1	All Stakeholders Policy Owner	Receiving Issues on Policies	As required
CP-2	Policy Owner Policy Manager	Evaluating Issues on Policies	1 week
CP-3	Policy Manager	Recommending Changes to the Policies	1 week

Roles: *The Stakeholders in the Policy Framework*

Policy Organisation Structure



Policy Roles and Responsibilities

A stakeholder is defined in the context of the Policy Framework as any person, organisation or group who is involved or impacted by the Policy Framework.

The Roles are classified into two types:

- **Named Roles**: consisting of existing committees and forums that play a part in the Policy Processes and for whom working with the IT Policies is a part of their responsibilities.
- **Assigned Roles**: these are Roles specific to the IT Policy Framework.

ICT Policy Committee: Named Role

This is an internal committee consisting of specific individuals (Chairman, Policy Manager) as well as key managers within the IT Department and other SBUs who will provide the inputs to direct the Policy Framework and its implementation.

The following is the suggestion of the most appropriate personnel and representatives for this committee:

- Chairman: the Chairman of the ICT Policy Committee is always the IS Manager, being the executive role within the committee.
- (optional) Vice-Chairman : stand-in for the IS manager
- Secretary: meeting management including agenda, invitations, attendance, minutes.
- ICT Policy Manager: a nominated individual who is a different person than the Chairman of the committee, being the operational role on the committee who will carry out the activities of the committee.
- Representatives from specified SBUs
  - Information Technology
  - Human Resources
  - Occupational Health and Safety
  - Community Safety

  - Legal
  - Records Management / Registry
  - Financial Management (specifically Asset Management)
  - Internal Audit and Risk Management (they will be on the committee as advisors until the ICT Policies are approved by the Council and thereafter will take on the role of independent auditing and compliance)

- External Representatives / Interested Parties
  - Office of the Mayor : as required
  - Local Labour Forum

The IT Policy Committee is the de facto "Owner" of the ICT Policy Framework. However in some cases the Owner is delegated to a particular individual or Role.

The ICT Policy Committee Chairman will always be the IS Manager or their delegate. If this Role is delegated the IS Manager will remain the authorised person and remains accountable.

The ICT Policy Committee is required to have its own constitution which defines its responsibilities and authority, and into which other municipal structures report into.

RECOMMENDATION: It is recommended that if possible, the ICT Policy Committee be constituted as a working committee of the Mayoral Committee. It is necessary that a Resolution of the Mayoral Committee will approve the Constitution of the ICT Policy Committee as well as any further changes to this Constitution.

The Constitution is required to include the following:

- The membership structure of the committee, including designated office bearers (Chairman, Vice-Chairman, Secretary), as well as portfolio members, each representing a specific constituency (as identified above within the list of members).
- The statement of responsibilities and representation for each of the members of the committee: for example, what each portfolio is required to do as a committee member, such as Legal: identifying the legal requirements for each of the Policy changes, and the Local Labour Forum who can comment on the policy changes required prior to these being discussed with the Mayoral Committee formally.

- The delegation requirements for situations in which an allocated member is not available and a delegate is required to attend in their place.

- The meeting: in terms of how and when the meetings are held, how these are notified.

- The standard agenda for the meetings, as well as the processes to include additional items onto the agenda.

- The reporting requirements in terms of who has to provide what reports for each meeting.

- How the ICT Committee is required to report into its parent committee. This should be in the form of a Policy Status Summary of one page.

ICT Policy Manager: Assigned Role

The ICT Policy Manager is a single individual who is given the primary responsibility for the management, administration and oversight of all of the ICT Policies. Their specific responsibility is to ensure smooth implementation of the Policies, Procedures, and Forms.

The ICT Policy Manager reports to the ICT Policy Committee and represents the implementation responsibilities of the ICT Policy Committee.

The ICT Policy Managers will delegate their work to other Roles under the ICT Policy Committee. It is likely that some of the specific Roles identified are conducted by the Policy Manager and are not delegated. The identification of these more specific Roles allows the ICT Policy Committee to allocate responsibilities to others in a structured manner.

The Policy Manager has three primary responsibilities:

- Communicating: Communication of the status of the policy framework to the ICT Policy Committee.

- Managing Change: Managing the Change Cycle in terms of receiving requests for change and translating these into changed Policies – following through the process until new updated Policies emerge to be implemented and enforced.

- Implementing Policies: Managing and be accountable for the daily operations of the Policies including implementation, education, enforcement, communications, violations and penalties, and configuration management.

Specification responsibilities of the ICT Policy Manager are:

- Reporting into the ICT Policy Committee in terms of the status of Policy implementation and enforcement – using a standard template for Policy Status Reporting.
- Oversight of all of the activities of all other Roles reporting into the ICT Policy Committee including the Policy Writers, Editors, Implementers, Enforcers, Reviewers, Communications, Educators, Configuration Manager.
- Work with the Policy Auditors (from the Internal Audit Unit).
- Liaise with the Policy Owners, who are specific members of the ICT Policy Committee who are focussed on one or more specific Policies.
- Receive inputs from the Policy Reviewers, Implementers, Educators and Enforcers in terms of issues concerning the implementation or usage of the policies.
- Receive inputs from users of the policy, all stakeholders who are subject to the policies, as well as line management, on issues which need to be attended to and then use these to enact the change processes as required.
- Receive inputs on violations and handle all escalations of violations through the HR departments in terms of disciplinary actions.
- Work with the Configuration Manager in terms of the current version and in terms of the change processes driven from the issues raised.

Mayoral Committee: Named Role

The Mayoral Committee will take the primary responsibility in recommending Policies for approval by the Council. To carry out their work they will liaise with the Local Labour Forum.

The Mayoral Committee will be required to identify the extent to which public participation/consultation may be required in formulating and receiving feedback on the ICT Policies. This does not include the employees, who are represented through the Local Labour Forum.

Local Labour Forum: Named Role

The Local Labour Forum is concerned with the impact of the policies on the employees whom they represent.

The Local Labour Forum represents the constituency of users within the scope of municipal employees.

Council: Named Role

The Council is the only official municipal body able to approve the ICT Policies.

The Council will approve these following recommendations made by the Mayoral Committee.

Policy Writer: Assigned Role

Policy Writers are individuals who write the policies using the inputs from the organisation as well as from external sources such as legislation, national policies and international best practices.

Their goal is to capture the content and justification for the policies and changes to these policies.

The specific responsibilities are:

- Receive the inputs concerning the changes to the policies
- Write the updates in order to preserve the content and intention of the policies

Policy Editor: Assigned Role

Policy Editors will turn the created policies into documents which are easy to read and clearly understood by those who are required to abide by them.

Policy Editors do not change the content or justification, but they change the words and sentences used to express these to ensure that all policies comply with best practices in terms of English style guidelines, for effective communication. They also ensure that the risk of misunderstanding and ambiguity are minimised through the words and sentences used.

The specific responsibilities are:

- Receiving the written policies from the Policy Writer
- Performing basic editing on the quality of the writing, using style guidelines that have been agreed upon
- Submitting the edited policies back to the Policy Writer

Policy Approvers: Assigned Role

Every individual, group and committee involved in the approval process is included in the definition of Approvers.

They are responsible for ensuring that the policies as written and edited meet the requirements of the municipality, and that they represent the views and aspirations of all stakeholder communities, in particular the Council, Management and Employees of the municipality. Visitors and the Community are included to the extent that they are impacted by the policies.

The specific responsibilities of this role are:

- Read the updated policies submitted for approval.
- Comment on the updated policies.
- Approve the updated policies for implementation.

Policy Configuration Manager: Assigned Role

This is a delegated responsibility of the ICT Policy Committee that is responsible for keeping the "original" copies of the policies and all related documents, in both physical and electronic form. They are also responsible for the distribution and control of the policies.

It is recommended that a single person on the ICT Policy Committee is responsible for configuration management, and that the responsibility is not shared with others.

The specific responsibilities of this role are:

- Maintain the original physical version of each individual policy, with clear identification of the current and historical versions.
- Maintain the master electronic versions of all policies (most likely using the Document Management System of the municipality as the basis).
- Maintain a list of all people who have physical copies of the originals.
- Keep track of all changes requested and issues concerning the policies.
- Distribute the physical copies of the documents with the updates.
- Distribute new physical files with all current policies.

Policy Communicator: Assigned Role

This role is responsible for the effective communication of the policies.

The Policy Communicator formulates the communication strategies to ensure that all employees have access to the policies through various means, including newsletters, the intranet, posters, seminars and workshops.

This Role does not physically distribute the policies, which is a specific responsibility of the Policy Configuration Managers.

The specific responsibilities of this Role are:

- Create the Communication Strategy for Policies.
- Develop specific Communication Plans for individual Policies as appropriate.
- Carry out the Strategies and Plans.
- Measure the effectiveness of the Strategies and Plans using quantitative and qualitative research (for example, by asking selected stakeholders the extent to which they are aware of the policies and their contents, and how to apply them).

Policy Implementers: Assigned Role

The implementation of policies includes the establishment of the processes for enforcement. This will include the establishment of the total environment for the enforcement.

The specific responsibilities are:

- Development of any Forms and Registers that are required to implement the policies.
- Develop any tracking requirements for monitoring and reviewing.
- Ensuring that the Policy Enforcers are trained in how to enforce (this is done by the Policy Educators).
- Ensuring that the stakeholders who are subject to this policy understand the policy sufficiently well to be able to work within its structure.

Policy Educators: Assigned Role

This Role has the function of training the Policy Enforcers about a Policy in terms of how to apply the Policy.

As required, this Role may also involve general training of selected employees on specific policies, as well as developing training materials and running train-the-trainer courses. The Policy Educators will help to establish policy awareness within employee orientation programmes and related workshops. It is assumed that the basic employee training will be conducted by existing training personnel and performed as part of orientation and re-orientation training programmes.

Specific responsibilities are:

- Development of training materials for stakeholder training.
- Development of training course for stakeholders training, including a train-the-trainer course.
- Development of training materials for Enforcer training.
- Conducting the training courses for stakeholders, for train-the-trainer and for Policy Enforcers, or alternatively supporting the existing trainers.
- Tracking the people who attend the courses.
- Reporting to the ICT Policy Committee in terms of the successes and failures on the course, and the extent to which the stakeholders have been trained.
- In particular, to report on problems with attendance at the courses, since this may impact on the risk of successful implementation.

Policy Enforcers: Assigned Role

Policy Enforcers are those who are responsible for ensuring that specific policies are enforced properly. There could be one specified Policy Enforcer for each individual policy.

Specific responsibilities are:

- To carry out the enforcement duties as identified within the individual policies.
- To ensure that Forms and Registers are completed as required.

- To report on any violations as soon as they occur as identified within the policy and its associated procedures, and to escalate these to the appropriate municipal structure.

Policy Reviewers: Assigned Role

Policy Reviewers are internal to the ICT Policy Committee.

Policy Reviewers will evaluate the effectiveness of the policies to ensure that they are delivering the benefits as expected. They will monitor the policy implementation in terms of the violations and penalties.

Policy Reviewers are responsible for receiving feedback on the policies and recommending changes to improve the effectiveness of the policies.

The Policy Reviewers should include personnel from municipal line management and the IS SBU.

The specific responsibilities are:

- Monitoring the usage of the Policies within the scope of their responsibility.
- Reviewing the policy implementation and enforcement in terms of the successes and failures, with improvements which may be considered for the next generation.

Policy Auditors: Assigned Role

Policy Auditors are purposely external to the ICT Policy Committee.

They are required to verify the compliance to the ICT Policy Framework through various assurance practices and processes. They perform both an auditing role as well as a consulting role.

They will be involved during the start up phase in order to ensure that the policies as created are suitably structured for auditing.

Following the start up phase they will be independent of the ICT Policy Committee and will perform audits as required within the scope of their responsibilities.

Specific responsibilities are defined by the Internal Audit unit itself. These are not specified within the scope of this ICT Policy Framework.

Policy Owners: Assigned Role

The Policy Owner is by default the IT Policy Committee.

Other personnel, mostly within the IS SBU, may be delegated the role of Policy Owner of one or more Policies. Policy Owners report to the ICT Policy Committee. It is expected that all Policy Owners are individual members of the ICT Policy Committee.

Each Policy Owner is required to keep track of the implementation and enforcement of the Policy during the Implementation Process and to report back on the following questions:

- Do the stakeholders have access to the policy?
- Have the stakeholders read and understood the policy?
- Is the policy being applied and enforced as planned?
- Are violations of the policy being dealt with appropriately?
- What improvements can be made to this policy to make it more effective?

The one key responsibility of the Policy Owner is to receive feedback relating to the policy and to record these for consideration during the Change Process.

Start Up: *Getting the Policy Framework Implemented*

Current Status

There are currently no approved ICT Policies within the municipality (as at November 2010).

Kick-Start Phase

The first phase in getting the Policy Framework implemented is to reach the point where the Council approve the initial set of policies.

The process for initial implementation of the ICT Policy Framework and the individual ICT Policies should follow this process:

- Research best practices and relevant legislation in terms of the ICT Policy Framework.
- Finalise the composition of the ICT Policy Committee both in terms of specific member portfolios and the individuals allocated to these portfolios within the start up phase.
- Develop the Constitution of the ICT Portfolio Committee indicating allocated responsibility and authority, committee structure, meeting administration, standard agenda, voting administration, as well as membership management and rules.
- Constitute the ICT Policy Committee within the authority structure of the municipality, in terms of it being recognised as a formal authority with defined responsibility and delegated authority, reporting into the Mayoral Committee. This will require a Resolution of the Mayoral Committee.
- Decide on the full complement of ICT Policies to be implemented.
- Draft the specific ICT Policies and the ICT Policy Framework (this is the document you are currently reading).
- Circulate the ICT Policy Framework to the ICT Policy Committee members and other relevant stakeholders and receive feedback.
- Create the final versions of the ICT Policies on the basis of feedback received.

- Public participation and interaction with the Local Labour Forum. This to be done in a workshop format with the ICT Policies being circulated in advance of the workshops.
- Formal submission to the Mayoral Committee for recommendation (as an "A" item on the Mayoral Committee agenda), and then onto the Council for approval.
- Once there is approval from the Council, then this becomes officially recognised and the implementation and enforcement phase will commence. This is the end of the Start Up phase.
- NOTE: Many of the ICT Policies can be implemented without prior approval of the Council, since these represent best practices and do not impact on the employees directly.

Initial Implementation Phase

The second phase of the Start Up is to implement the Policies as an integral part of the operation of the municipality.

This implementation will include all of the activities as identified within **Process IP: Implementing Policies**, as outlined below. However, whereas those processes are intended to be implemented on one policy at a time, during this Initial Implementation Phase it is necessary to carry out these IP process on all Policies simultaneously.

The combined implementation of all of the Policies at once will create a far more complex implementation environment, and this is to be structured as a special project.

The following approach should be used to support the implementation of all of the Policies:

- The Outcome is the successful implementation of all of the Policies as identified within the Policy Framework as have been approved by the Council.
- The Outcome also includes the implementation of the Policy Management Processes as outlined in this Policy Framework to ensure that this is sustainable.
- The Outcome also includes the commencement of the Monitoring and Review, as well as the Policy Auditing Processes and the regular communication of Policy Status Reports to the ICT Policy Committee, which in turn provides a Policy Status Summary to the Audit Committee.

- The Implementation is prepared for each of the Policies in terms of how each Policy will be carried out in terms of the Procedures applicable for each Policy. This will include the development of Forms, Registers and other data collection instruments which will assist in the management of the Policies.
- General Communication on the Initial Policy Implementation will be carried out to inform all stakeholders of the implementation and to prepare them for these Policies.
- The initial training will take place with the Enforcers in order to prepare them to enforce their own specific policies. Where possible this will be done in groups.
- The implementation of the Policies will be prioritised to ensure that this does not place too much of a burden on the implementation team.
- A cooling off period will be provided for all Policies that involve users of the ICT facilities, most especially in terms of acceptable usage.
- The ICT Policy Committee will monitor all implementations and provide ongoing feedback and support during this time.

Once the Initial Implementation Phase has been completed, then further changes will continue as part of the Change Cycle.

Risk: *What are the Risks in Implementation?*

NOTE: This is a detailed description of the Risk Management processes to be used as identified in Process IP-7.

It is important to understand the inherent risks within the introduction of the ICT Policies so that mitigations can be planned in advance of their occurrence.

The risks identified here are drawn from SANS Institute and whereas they apply primarily to policies in information security, they are generally applicable in all ICT Policy structures.

These risks should be reviewed on a regular basis by the ICT Policy Manager and presented for consideration to the ICT Policy Committee.

These risks occur both during the Initial Implementation Phase as well as in the ongoing Policy Management Process.

Risk Factor and Risk Appetite

Each Risk is analysed in order to determine a Risk Factor, which is the product of the Impact Factor (1-3) and the Probability Factor (1-3).

The Risk Factor is on a scale of 1-9.

The Risk Appetite is the amount of Risk that the ICT Policy Committee is prepared to bear before considering preventative measures.

Risks below the Risk Appetite can be handled by means of counter-measures as and when they occur.

Risks above the Risk Appetite are required to be handled by counter-measures at the time they are identified and before they have actually occurred.

As an example, consider that a specific policy is critical and there is a risk that this may not be enforced properly. The Risk Factor is calculated at 6, which is above the Risk Appetite which is set at 5. As a result, the ICT Policy Committee will require that an alternative enforcement process is implemented as a backup in case the recommended enforcement approach fails.

Risk Log

Description

The Risk Log contains a list of all identified Risks, with their associated probability, impact and proximity, and an outline of proposed counter-measures.

Contents

Each entry in the Risk Log identifies a single Risk and must contain the following information:

- Risk Number : a sequential number identifying the sequence in which this Risk is identified.
- Date Identified : the date on which this Risk was originally identified.
- Who Identified : the person who identified the Risk.
- Risk Owner: the person who has been given the responsibility to keep an eye on this Risk and to report on Impact and Probability.
- Date Analysed : the date on which this Risk was last identified.
- Impact : what will be the impact if this risk occurs.
  - 1 : Little impact
  - 2 : Medium impact
  - 3 : Large impact
- Probability : what is the likelihood of this risk occurring:
  - 1 : Low probability
  - 2 : Medium probability
  - 3 : High probability
- Proximity : how soon in time is this likely to occur.

NOTE: There are no hard and fast rules in terms of the allocation of the Impact Factor and the Probability Factor.

Owner

ICT Policy Manager

Change Triggers

The Risk Log is changed by two processes:

- Risk Identification Process : in which new Risks are added to the Risk Log.
- Risk Analysis Process: in which the risks are assessed in terms of their impact and probability, and in which counter-measures are considered and updated.

Where Used

This is used by the ICT Policy Committee to assist with their regular risk assessment.

Risk Identification Process

Trigger

A new risk is noticed by any stakeholder of the ICT Policies and Procedures.

Process Owner

Any stakeholder initiates this process. It is then passed onto the ICT Policy manager.

Inputs

Any event, incident or observation that may impact on the success of any part or the whole of the ICT Policy Framework.

Outputs

A new risk is added to the Risk Log.

Steps

Seq	Activity	Who	Duration
1	A stakeholder alerts the ICT Policy Manager about a situation which threatens any specific ICT Policy, Procedure, Standard or Form, or which threatens the ICT Policy Framework as a whole. There is no specific reporting format for this, and it is recommended that this be done in writing to serve as the start of the process for tracking purposes.	Requestor	
2	Adds the Risk to the Risk Log.	ICT Policy Manager	24 hrs
3	Obtain additional information to determine the probability of the Risk, as well as the Impact and Proximity. Determine the Risk Factor as Impact * Probability.	ICT Policy Manager	24 hours
4	Update the Risk Log to indicate the Risk Factor.	ICT Policy Manager	0
5	Recommend counter-measures to apply for the eventuality that this Risk materialized. There may be more than one counter-measure recommended.	ICT Policy Manager	
6	If the Risk Factor is beyond the Risk Appetite, then notify the ICT Policy Committee along with the Counter-measures. The ICT Policy Committee will elect a Risk Owner for the Risk who will be responsible to keep an eye on the Risk.	ICT Policy Manager/ ICT Policy Committee	0

Risk Analysis Process

Trigger

This should be conducted monthly, prior to the ICT Policy Committee meeting.

Process Owner

This is conducted by the ICT Policy Manager on behalf of the ICT Policy Committee.

Inputs

Risk Log

Outputs

Updated Risk Log

Steps

Seq	Activity	Who	Duration
1	The ICT Policy Manager examines the Risk Log and requests each of the Risk Owners to provide an updated score for Impact and Probability as well as to identify the Proximity, if this is relevant.	ICT Policy Manager Risk Owner	monthly
2	Updates the Risk Log.	ICT Policy Manager	
3	Prepares a Risk Report and presents this to the ICT Policy Committee.	ICT Policy Manager	
4	Updates the Risk Log to indicate the Risk Factor.	ICT Policy Manager	

Summary of Key Initial Risks

At the time that this ICT Policy Framework is being initially adopted, we are recommending a number of Risks be considered for initial inclusion into the Risk Log.

It is important to note that these are NOT events that have occurred, but rather are suggested for consideration due to their potential impact, and that formal counter-measures should be planned in advance in case they become a reality.

RISK: Policies not taken seriously

MITIGATION

- Management backing beyond the approval within the Council.
- Strong buy-in from the Local Labour Forum.
- Good awareness campaign both before and during the implementation.

RISK: Lack of timely reviewing feedback

ISSUE

The reviewers must be competent to review the policies prior to their submission and to provide useful feedback and comments based upon a critical evaluation of the Policies. This must be done prior to submission of the Policies for approval.

MIGITATION

- Strong chairman of the ICT Policy Committee.
- Selecting reviewers who have the time to review the Policies.
- Ensuring that reviewers know what is required of them.
- Ensure that all reviewers are able to respond in a timely manner and that there are not delays.

RISK: Policy is unclear

MITIGATION

- Ensure that the Policy is directed at well-defined situations.

- Ensure that the Policy is written in language that is easy for everyone to understand.

RISK: People get upset by the new policies

ISSUE

The policies will limit the activities of the employees and will prevent them from doing things which they have been used to, such as accessing specific web sites that are banned under the new policy. This may create tensions that need to be mitigated.

MITIGATION

- Ensure that the Local Labour Forum are involved.
- Ensure that all stakeholders are consulted throughout the process so that there are no surprises.
- Ensure that all stakeholders are able to voice their opinions in the Initial Implementation Phase as well as during the ongoing Policy Management Process.

Scope: *What is the Structure and Content?*

The ICT Policy Framework is essentially concerned with the set of Policies that are required to be maintained. The Policies represent the core of the Policy Framework, with the Roles and Processes being used to position the Policies in an organisational structure and a management environment.

One key element of the Policy Framework is the Scope, in terms of the range of Policies which fit into this ICT Policy Framework.

How are the Policies Structured?

There is a natural overlap between the various ICT Policies, and it is important to have a solid basis to determine which combination of policies are collectively sufficient and useful to achieve the ends of this Policy Framework.

The decisions to be made are:

- What behaviours fall within the scope of the ICT Policies? (In other words, for which behaviours is a Policy the most effective means of control).
- How should Policies be organised and grouped?
- What specific Policies are required to provide a sufficient control environment, when should a large policy be split into a smaller one, and when should smaller policies be grouped into a larger one?
- How should Policies be subject to priority in the event of there being conflicting policies for a given situation?

The approach taken in this Policy Framework has been to identify the policies required using the following guidelines and expected outcomes:

- A strong match between the situations to which the policies apply and the policies themselves.
    - OUTCOME: For each situation in which a policy applies it is clear which is the right policy to apply. There is minimal ambiguity.
- A linkage between Policy Ownership and the Policies.

  - OUTCOME: There are no situations in which there is multiple ownership of policies as far as is possible.

- Sufficiently small to ensure that it is easy to read and understand as a stand-alone document for a specific situation.

  - OUTCOME: Minimal effort in training and education as well as reduced misunderstandings in compliance.

- Sufficiently large so as to avoid the problem of many smaller policies which are similar to one another.

  - OUTCOME: 10-20 Policy documents in total.

- The need to separate common policies as a reference point for the others. For example, overriding policy statements, such as the legal requirements in terms of the effective usage of ICT resources.

- The need to be clear and understandable throughout the Policies, using language which any stakeholders should be able to readily understand.

  - OUTCOME: Minimal effort in training and education as well as reduced misunderstandings in compliance.

The Categories of Policies

The Categorisation structure is under the control of the ICT Policy Committee and is used to group the Policies into useful subsets for allocating ownership and responsibility for implementation, enforcement, monitoring and review.

The Policy Owner is the person allocated to keep an eye on each specific policy and to report on their continued relevance and applicability in the light of changing external (to the municipality) environment and internal circumstance.

Within each Policy Category there is a set of specific Policies.

This Policy Framework Document provides an overall list of the Policies to be included, but does not explain these Policies in detail. Each of these Policies is then provided in a separate document.

Over time Policies may change, new Policies may be introduced, and Policies may be merged or split.

Category 01 Policy Administration

- Dealing with the development, management and installation of the policies.
- Provides a Policy Framework, which is unique in the country for Municipalities.

Category 02 Acceptable Use

- Policies for all situations that concern acceptable use of the ICT Assets.

Category 03 Communications

- Dealing with email and Internet communications in particular.
- These include disclaimers for usage with email messages sent out and for users of the municipal web site.

Category 04 Data and Information

- Including the definition and handling of "sensitive" information as well as retention requirements for official records.

Category 05 Information Security

- This concerns the protection of data and information as well as security controls for physical sites and electronic access to the ICT resources.

Category 06 Equipment

- This covers the various types of equipment and proper treatment including laptops and audiovisual equipment.

Category 07 Facilities

- This includes guidelines and policies for running the ICT facilities of the municipality including servers and networks.

Category 08 Applications

- These guidelines and policies concern the software used within the municipality – how they are built, maintained and managed.

Category 09 Disaster Recovery

- This is an ICT-specific element of the municipal disaster management strategy and plan. This includes areas not covered in the general disaster recovery plan.

Category 10 Training and Support

- This concerns the minimal standards for computer user proficiency as well as the management of a support desk.

Category 11 Green ICT

- This is an emerging concept in ICT in general and in government in particular. These policies help make the municipality an environmentally-friendly organisation and make its contribution to reduction in global warming.

Category 12 Contractors and Suppliers

- This last category deals with guidelines on the management of contractual relationships with third parties.

Process: *How are Policies Managed?*

This Policy Framework adopts a cyclic approach to the process of policy management.

The Policies are maintained within a Master Policy File, which contains the original electronic and physical copies of the Policies, and which is maintained under strict configuration management. This Master Policy File is also considered to be one of the Information Resources as maintained by Policy IT-01-03 Register of Information Resources.

This Policy Process is structured as a formal process with checks and balances to ensure effective execution by the individuals with the appropriate level of authority. There are three high-level processes within the cycle:

- (AP) Approving Policies : writing, editing and approving the policies prior to their implementation and enforcement.
- (IP) Implementing Policies : introducing the policies, implementing, communicating and enforcing policies – this also includes regular reviewing and auditing.
- (CP) Changing Policies : receiving feedback, performing impact analysis, proposing changes.

Policy Configuration Management

Master Policy File

The Information Systems SBU must maintain the complete set of policies, including current and archived versions, using an effective configuration management or document management system.

This set is referred to as the Master Policy File and should be managed as a single unit as an Information Resource.

A printed version of the current policies and forms of the Master Policy File is maintained by the IS Manager. This is maintained in printed form in Office XXXX and is stored under the File TTTTT. A copy of this is maintained within the Records Department.

This printed version will be used as the primary reference source in disputes concerning which is the current version.

The Master Policy File is maintained by the Policy Manager.

An electronic copy of each Policy is maintained in read-only form on the folder "Master ICT Policies and Procedures" on the municipal file server. All of the files are maintained in read-only PDF files.

This Master Policy File in electronic form is accessible through a single web page which provides hyperlink access to all of the current policies.

Each Policy has a unique Policy Code which is of the form:

- POL-IT-aa-bb-nnn
- Where
  - POL-IT = Policies for IT
  - aa = the Policy Section
  - bb = Policy Number within the Policy Section
  - nnn = version number

Master Policy File Sections

The Master Policy File is divided into Policy Sections which are structured into the Categories as identified under the "Scope" heading in this document.

Policy Structure and Template

Each Policy must be structured in accordance with the standard policy template, which is the structure as maintained within the document IT-01-04 Policy Checklist.

Each policy must contain the following information:

- Policy Section : which section it is in.
- Policy Number : which number within the section.
- Title : the short title of the Policy.
- Scope : the scope of situations and activities which fall within the Policy.
- Purpose: which outlines the primary purpose(s) of this Policy within the Policy Scope.
- Applicability: the situations to which this policy applies, and the people / roles to whom the policy applies and who are involved in the procedures.
- References: a list of other documents and articles which can be used as the basis for the Policy and which inform the Policy.
- Policy : the statement of the Policy, divided into sections as required.
- Procedures: a statement of the steps to be followed in each procedure, including the forms that are used to support the procedures.
- Forms / Registers / Logs: a reference to external forms used and registers and log maintained for the policy.

Copy Policy Files

A set of Copy Policy Files are maintained, where each is a duplicate of the printed Master Copy File maintained by the IS Manager.

A list is maintained of the people who keep Copy Policy Files. This is called the Distribution List.

Whenever there is any update to the Master Policy File, then a printed copy of the Policy will be provided to everyone on the Distribution List who will then update their Copy Policy File by inserting the new/updated Policy.

The Copy Policy Files are included within the scope of the Audit Procedure.

Process AP: Approving Policies

This process involves the activities required to produce approved policies.

- Inputs: Requests for Changes to Policies
- Outputs: Resolutions that Approve the Policies

This includes the following sub-processes:

- Writing Policies
- Editing Policies
- Validating Policies
- Approving Policies

Sub-Process AP-1: Writing Policies

Purpose

The policy needs to be written to document the needs of the municipality. In order to effectively enforce a policy it must be written and based upon an assumed verbal understanding.

When changes to a policy are required, the first step is to document the changes to the existing policy.

Responsibility

Policy Writer.

Activities

Using the Policy Template and/or Existing Policy, write the paragraphs which indicate the updated requirements.

Inputs

Existing policy where an approved and enforced policy exists.

The Policy Template.

Outputs

The New or Updated Policy, reflecting the full content as required.

Quality Control

All elements of the requirements should be included in the new or revised policy.

Sub-Process AP-2: Editing Policies

Purpose

Policies must be read and understood by all whom they affect. To communicate the right intentions, the words, sentences and paragraphs of a Policy Document should be drafted by an expert.

Responsibility

Policy Editor

Activities

The policies as written must be edited in order to ensure that they conform to the guidelines for effective written communication.

Among the key areas of concern are:

- Minimal ambiguity in the usage of words and phrases.
- Easy to read sentences.
- Fully reflecting the original intent of the policy.
- Concise and to the point.

Inputs

Policy Style Guidelines.

Written Policy Document from AP-1.

Outputs

Edited Policy Document.

Quality Control

The Edited Policy Document must meet the guidelines for effective communication as outlined in the Policy Style Guidelines.

Sub-Process AP-3: Validating Policies

Purpose

Prior to seeking formal approval, it is important to obtain informative reviews from key stakeholders.

Responsibility

IT Policy Committee, perhaps in conjunction with Local Labour Forum.

Activities

The Edited Policy Document is reviewed by all members of the IT Policy Committee and relevant stakeholders.

If this is found to be acceptable it is then passed on to the Mayoral Committee for Approval.

Inputs

Edited Policy Document from AP-2.

Outputs

Validated Policy Document.

Quality Control

There are no formal guidelines for this quality check, and it is up to each individual member of the IT Policy Committee to ensure that they provide the feedback from their own perspective and functional/ technical background.

Sub-Process AP-4: Approving Policies

Purpose

Before a Policy can be implemented and enforced it must be approved by the Council, who is the only body mandated to approve new policies.

Responsibility

Policy Approvers.

In the case of the municipality this includes the Mayoral Committee, the Local Labour Forum, and the Municipal Council.

Activities

This process is outside of the control of the IT Policy Committee.

Once a policy update is submitted to the Mayoral Committee this will then be passed through the process until this is either rejected or is approved by Resolution of the Council.

The following outcomes are possible:

- Approved as presented, without changes.
- Approval with recommended changes effected before implementation.
- Rejected, together with identification of the areas which are preventing approval.

No outright rejection is acceptable, since the IT Policy Committee will need to be informed of the areas of weakness, in order to proceed with the review and amendment of the document for re-submission.

If it is rejected, then this is returned to the IT Policy Committee who will then request the Policy Writers to make the necessary changes.

If it is accepted with changes, then the Policy Writer must make these changes. The Policy Editor must edit the changes, and the IT Policy Committee must ensure that the changes as made conform to the Resolutions of the Council.

Inputs

Validated Policy Documents.

Outputs

Approved Policy Documents, perhaps with changes as requested by Resolutions of the Council.

Quality Control

The Resolutions reflect approval of the Policy Documents.

All changes as reflected in the Resolutions have been made and these changes validated by the IT Policy Committee.

Process IP: Implementing Policies

Once a policy is approved, including approval of changes to existing policies, it is then required to be implemented within a time frame as identified in the approval.

This is affected by the following sub-processes:

- Communicating the Policies
- Training on the Policies
- Implementing the Policies
- Enforcing the Policies
- Monitoring and Reviewing the Policies
- Auditing the Policy Implementation

Sub-Process IP-1: Communicating the Policies

Purpose

It is essential that each person affected by a policy is informed about the policy. If the individuals are not aware of the policies that they must abide by then this threatens the effectiveness of the policies.

Responsibility

Policy Communications.

Activities

Each Policy is communicated to the relevant stakeholders using one or more appropriate methods.

The method of communication is indicated within the policy itself.

The suggested methods for communication are:

- Intranet.
- Printed Policy Manual made available at particular points, for example one within each SBU.
- Training within the Orientation and other training courses.

- Posters provided at key locations, such as in the lifts, passages and other municipal offices, as well as in entrances to controlled locations.

Inputs

Approved Policies

Outputs

Communication activities for ICT Policies in general.

Communication activities for specific ICT Policies which require additional or specific implementation interventions.

Quality Control

The Communication Plan is implemented as per the policies.

The stakeholders demonstrate knowledge of the policies from the communications provided. Affected users should know that the policies exist, and where to obtain the details of the policies. The actual content and knowledge of the policies are left to the training interventions.

Sub-Process IP-2: Training on the Policies

Purpose

Providing the Policies alone is insufficient to ensure compliance. It is also important that the substance of the policies are introduced into the existing training programmes for employees, as well as within specialised ICT Policy Training courses.

Responsibility

Policy Educator

Activities

- Develop educational materials, including course notes, for each of the policies.

- Develop a train-the-trainer course structure.

- Providing the training to the trainers and to the enforcers as required.

Inputs

Approved Policies

Outputs

- Training Materials (new/updated).
- Train-the-Trainer Course (new/updated).
- Trained Trainers.
- Trained Enforcers.
- Assessments to gain evidence for the familiarity with the Policies.

Quality Control

- Training incorporates the complete substance of the Policies.
- Users who have been trained demonstrate sufficient knowledge of the Policies.
- The trainers are able to perform the training.

Sub-Process IP-3: Implementing the Policies

Purpose

The Policies are not intended to be purely documents which are left in files and on web sites. Each of the policies is intended to be a living process which is implemented in order to improve the effectiveness of the goals of the procedures.

Responsibility

Policy Owner

IT Policy Committee

Activities

- Identify all changes to the existing policies.
- Implement the new policies in terms of new Forms and new Procedures.
- Update the training materials as required.

Inputs

- Approved Policies

Outputs

- Change Forms / Procedures

Quality Control

The changes to the Forms implement the substance of the changed Policies.

Sub-Process IP-4: Enforcing the Policies

Purpose

Once the Policies are implemented, they need to then be enforced to ensure that all those stakeholders impacted by the policies comply, and that violations are treated using the right disciplinary procedures and penalties.

Responsibility

Policy Enforcer

Activities

This is the person who is directly responsible for the enforcement of the policy. This could be anyone, and each individual Policy should have its own specific enforcer.

Some policies require constant enforcement, and others may require random or regular checks.

For example, a policy on the movement of equipment will require documentation to be handled to support the movement, and someone must be responsible for this. However, a policy on appropriate usage does not require a person to constantly check, but rather conduct random audits of the users.

The following specific activities will be required:

- Completion of the Forms by the people who need to comply with the Policies.
- Approval of the Forms by the relevant personnel as required.
- Record-Keeping of the completed forms.
- Keeping a register of Violations and Incidents relating to the procedures.

- Passing on to Human Resources incidents that warrant further attention for disciplinary purposes.
- Recording the disciplinary actions taken.

Inputs

- Approved Policies

Outputs

- Enforced Policies.
- Completed Forms.
- Logged Forms.
- Register of Incidents and Violations.
- Record of Penalties Applied.

Quality Control

- Forms and other parts of the Policy are implemented as per the Policy.
- Record-keeping is up to date.
- Violations and other Incidents are recorded properly.
- Penalties are applied consistently and appropriately.
- Penalties are recorded.

Sub-Process IP-5: Monitoring and Reviewing the Policies

Purpose

Each of the Policies will need constant attention in terms of monitoring their effectiveness and reviewing them.

These are intended to monitor and review the processes without having to wait for the internal audit processes.

This is essentially a compliance assurance process.

Responsibility

IT Policy Committee and nominated delegates.

Activities

- Conduct regular reviews of the policies.
- Discuss the policies with stakeholders in order to get feedback.
- Check that the policies are being implemented correctly.

Inputs

Implemented and Enforced Policies

Outputs

- Records of Reviews.
- Feedback to pass to Changing Policies process.

Quality Control

- Reviews are conducted and recorded regularly.
- Problems with the implementation and enforcement of the policies are noted and corrected.

Sub-Process IP-6: Auditing the Policy Framework and Policies

Purpose

Internal Audit must ensure that the municipality comply with its internal policies and procedures, as well as with relevant legislation.

Responsibility

Internal Audit

Activities

- Checking that the policies are being implemented and enforced correctly.
- Reporting on any problems identified, to the Audit Committee.

Inputs

Existing Policies as Implemented and Enforced.

Outputs

- Report on compliance with the policies, in terms of implementation and enforcement.

Quality Control

- Quality is managed through the processes within Internal Audit.
- This process may be quality assured by the external auditors.

Sub-Process IP-7: Risk Management

Purpose

There are considerable risks associated with ICT usage and resources, and these must be managed through the formal risk management functions of the municipality.

These risks are critical to contain as part of the ongoing operation of the municipality and are reported to the Audit Committee.

Responsibility

Risk Management

Activities

- Comment on new policies and updates in terms of Risk Management requirements.
- Development of ICT Risk Framework including identification of key risks and the process of evaluation of their probability and impacts.
- Determination of the Risk Appetite for the municipality in terms of each identified Risk.
- Determining the Risk Response for each identified Risk, including mitigation and other counter-measures.
- Analysis of incidents from a risk perspective. For example, incidents concerning attempted security breach or virus infections.
- Risk Reporting to the ICT Policy Committee as well as to the Risk Committee.

Inputs

Existing Policies as Implemented and Enforced.

Outputs

- Report on risk analysis and management
- Report on risk profile.

Quality Control

- Risks are identified and used for preventative measures in improving the risk profile within the risk appetite.

Policy Issues Log

Description

A Log of all Policy Issues indicating relevant information such as who raised the issue and when, what is the substance of the issue, what type of issue it is, and how this was decided on.

Contents

Each entry in the Policy Issues Log is for a single Policy Issue and must contain the following information:

- Project Issue Number : a sequential number identifying the sequence in which this issue has been received
- Date: the date on which this Policy Issue was originally raised
- Creator : who raised the issue
- Type : the type of the issue
- Priority : the priority of this issue
- Action : what action taken
- Status : the status of this issue

Owner

ICT Policy Manager

Change Triggers

The Policy Issues are changed by the CP processes:

Where Used

This is used by the ICT Policy Committee to consider the issues raised and to recommend the action to be taken.

Process CP: Changing Policies

The Change Process within the total Policy Management Process Cycle is concerned with the manner in which changes are considered and recommended before the next cycle of writing begins.

The sub-processes involved with the Changing Policies process are:

- Receiving Issues on Policies
- Evaluating Issues on Policies
- Recommending Changes to Policies

Sub-Process CP-1: Receiving a Policy Issue

Purpose

Policies are in a constant state of change as they are applied and as experience is gained in applying and enforcing them.

The first step in the process of change is to record issues in terms of all form of feedback on the usage of policies and any other comments from all stakeholders.

Responsibility

All stakeholders who are providing feedback, comments and requests for change.

Policy Owner: receiving the issues and recording this.

Activities

- Feedback is sought actively from all stakeholders on a regular basis in terms of all policies. It is important as part of the communication plan for the policies that all stakeholders are informed about the change process and in particular that this starts with the Policy Issue Form.
- The Policy Issue Form IT-01-50 is completed by the stakeholder and provided to the Policy Manager.
- The Policy Manager will allocate the next sequential number to this Issue and will write this into the Policy Issues Log as well as writing this onto the form itself.

Inputs

Implemented and Enforced Policies

Outputs

- Record of the feedback and the changes requested.

Quality Control

Feedback, comments and requests for change are recorded as Policy Issues where appropriate.

Sub-Process CP-2: Evaluating a Policy Issue

Purpose

Once a Policy Issue has been received concerning any individual policy, it is necessary to determine the appropriate action to take.

Responsibility

Policy Owner

ICT Policy Manager

Activities

Each of the individual Policy Issues must be classified into various types:

- Request for Change
- Report of Problem in Implementation
- Report of Problem in Enforcement
- General Comments
- External Influences which may impact the Policy
- Other

Once a Policy Issue has been classified then the Issue is evaluated in terms of actions that should be taken and an impact analysis made for the Policy or Policies concerned.

Inputs

A New Policy Issue

Policy Issues Log

Outputs

- The evaluation of the Policy Issue and recommendation on changes.

Quality Control

- The most appropriate classification is given.
- The most appropriate action is recommended
- The timing is appropriate for this activity.

Sub-Process CP-3: Approving a Recommendation to Change a Policy

Purpose

Following the recommendations on actions that will impact the Policies it is important to approve these before actually making the changes.

This requires establishing the details of the changes to be made, which are then fed back into the Policy Writing process.

Responsibility

Policy Owner

ICT Policy Committee

Activities

- If there are changes to be made, then these should be formulated as changes to the existing policy which they affect, or should be structured as details for a new policy.
- These are approved by the ICT Policy Committee.
- These are then provided to the Policy Writer to commence the next cycle in the Policy Management Process.

Inputs

Current Policy.

Policy Issue including recommended changes.

Outputs

Approved changes to be implemented into the Policy.

Quality Control

- The approved changes implemented into the next round of policy changes.

NB: This policy shall be effective upon approval by Council and shall be reviewed after three years from the date of approval or should the need arise.

Approved/ Disapproved

28/05/2018

Cllr. Paya ME

Date

Mayor

* * * END OF DOCUMENT * * *