ABAQULUSI MUNICIPALITY

Draft ICT Policy

ICT Section

Corporate Services Department

Rev. 1.2

Contents

ACTIVITY MONITORING POLICY AND PROCEDURE

1. TABLE OF CONTENTS

1. INTRODUCTION

AbaQulusi Municipality considers all electronic information transmitted over the organisation's network to be private and confidential. Network and system administrators are expected to treat the contents of electronic information as private and confidential. Any inspection of electronic files, and any action performed following such inspection, will be governed by all applicable statutes and policies.

2. OBJECTIVES

AbaQulusi Municipality's communication systems will primarily be used for business purposes. All messages and information, which are sent through the internal computer and communications systems, will be deemed the property of AbaQulusi Municipality.

Hence, this Activity Monitoring Policy document deals with operational monitoring and security events monitoring. As such, AbaQulusi Municipality reserves the right to monitor, access, retrieve, read, and / or disclose employee communications at any time when:

- A legitimate business need for such action exists;
- The involved employee is unavailable and timing is critical to a business activity, provided the employee has given prior consent for such action;
- There is reasonable cause to suspect criminal activity or material violation of company policies; and
- Monitoring is required by law, regulation, or a third-party agreement.

3. SCOPE

This policy equally applies to all individuals that have, or may require, access to AbaQulusi Municipality's information resources residing on key financial, operational computer applications, databases and operating systems and those with the responsibility for maintaining these information resources.

4. POLICY and PROCEDURE

4.1. Administrator and Operator Logs

4.1.1. The ICT Department is responsible for any information processing and must keep a log of all operational and production activities (see Appendix A and Appendix B).

- This log must include:
  - Date/time of activity;
  - Activity description;
  - Error handling and action/resolution, if applicable;
  - Verification of proper operational procedure; and
  - Name and account of the operations person.

4.1.2. The ICT Manager must ensure that operations logs are reviewed weekly for consistency and proper documentation.

4.1.3. Operations logs must be archived and available for independent verification.

4.1.4. Area's to be monitored include and are not limited to the following:

- Review Application Logs for Error Events
- Review All System / Application Event Logs for Warnings
- Record Errors and/or Warnings
- Respond to Failures / Problems
- Systems are started or stopped
- Input or output devices attached or detached

4.2. Audit Logging

4.2.1. The ICT Manager must ensure that unit logs record the following information on all business critical resources if the business requirements determine them to be relevant:

- User IDs;
- Dates/times and key events;
- Unsuccessful resource access attempts;
- System configuration;
- Privilege uses;
- System and application utilities use;
- The files accessed and type of access;
- Network addresses and protocols used;
- Access control system alarms that were triggered; and
- The activation and de-activation of security protection systems.

4.2.2. The ICT Manager must review audit logs on a monthly basis and sign-off as evidence of the review (see Appendix B).

4.2.3. The Director Corporate Services must provide approval after the logs have been reviewed by the ICT Manager.

4.2.4. The ICT Manager must ensure that evidence of the review is retained.

4.3. Clock Synchronisation

4.3.1. The ICT Department must ensure that information processing devices must be set to an agreed standard and synchronised with an agreed accurate time source.

4.3.2. A procedure must be established that verifies the accuracy of the system time and provide corrections as needed.

4.4. Fault Logging

4.4.1. The ICT Manger must ensure that system faults and errors are logged and analysed to determine the appropriate course of action to be taken. The level of logging required must correspond to the risk associated with the system. Logs must be reviewed weekly for consistency and proper documentation. These logs must be archived and available for independent verification (see Appendix A).

4.4.2. The ICT Manager must ensure that open errors or issues remain open until they are satisfactorily resolved. Resolved faults and errors must be reviewed to determine if they have been properly authorised and to determine if security controls have been compromised.

4.5. Monitoring System Use

4.5.1. Auditing must be set up for both successful and failed logons, security logs must be reviewed on a monthly basis by the ICT Manager. All security incidents identified must be recorded in the System Monitoring Log Sheet and signed-off by the Director of Corporate Services (see Appendix B).

4.5.2. The ICT Manager must ensure that monitoring for unauthorised system access captures the following details:

4.5.2.1. Failed or rejected actions performed by users;

4.5.2.2. Failed or rejected attempts to access data or resources;

4.5.2.3. Policy violations and notifications from perimeter defense devices; and

4.5.2.4. Intrusion detection system alerts.

4.5.3. IT risk assessments for the level of monitoring required by systems will determine:

4.5.3.1. The criticality, sensitivity and value of the system's information and processes;

4.5.3.2. The potential impact of system compromise from past experience;

4.5.3.3. The level of system interconnection; and

4.5.3.4. The impact of logging capabilities being de-activated.

4.5.4. The ICT Manager must ensure that monitoring for the use of privileged operations occurs during the following instances:

4.5.4.1. Systems are started or stopped;

4.5.4.2. Input or output devices are attached or detached; and

4.5.4.3. Changes and attempts to change security settings and controls.

4.5.5. The ICT Manager must monitor the use of privileged accounts. This must be reviewed further and signed by the Director Corporate Services.

4.5.6. The ICT Manager must ensure that monitoring for system alerts and failures capture the following details:

4.5.6.1. Alerts or messages from consoles;

4.5.6.2. Exceptions in system logs; and

4.5.6.3. Alarms generated by network management devices or access control systems.

4.5.7. The ICT Manager must ensure that monitoring for system access captures the following details:

4.5.7.1. The ID of the user;

4.5.7.2. The date/time of key events;

4.5.7.3. The type of event;

4.5.7.4. Failed access to files; and

4.5.7.5. The programs or utilities used during access.

4.5.8. The level of system monitoring for users must be determined by a risk assessment by the ICT Manager. The level of monitoring must be in compliance with all applicable laws and regulations.

4.6. Protection of Log Information

4.6.1. The ICT Manager must ensure that security controls are implemented to protect against unauthorised log manipulation and tampering.

4.6.2. Security controls must protect against:

4.6.2.1. Alterations to recorded messages;

4.6.2.2. The deletion or editing of log files; and

4.6.2.3. Storage capacity of log files being exceeded.

5. ENFORCEMENT

Non-compliance, violation and disregard of this policy by any AbaQulusi Municipality employees, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual's employment contract, depending on the circumstance and the gravity of the transgression. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the individual and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the individual.

6. APPENDICES

6.1. Weekly Activity Monitoring Checklist

6.2. Monthly Activity Monitoring Checklist

Appendix A – Weekly Activity Monitoring Checklist

Weekly Activity Monitoring: Tasks Checklist	Date:
Administrator and Operator Logs	**Tick if Completed**
Review Application Logs for Error Events	
Review All System / Application Event Logs for Warnings	
Record Errors and/or Warnings	
Respond to Failures / Problems	
Systems are started or stopped	
Errors on Backups	

SIGN-OFFS

Performed by:		**Designation:**	
Signature:		**Date:**	
Where there any Security Incidents? (Yes/No). **If yes, provide details and Incident No. and resolution**			
Director Corporate Services Signature:		**Date:**	

Appendix B – Monthly Activity Monitoring Checklist

Monthly Activity Monitoring: Tasks Checklist				
Review of Security Logs	**Date**	**Performed by:**	**Designation**	**Signature**
Unsuccessful system access attempts				
System Configuration changes				
Privilege access uses				
System and application utilities use				
Failed access to files				
Exceptions in firewall logs				
Access control system alarms that were				
The activation and de-activation of security				
Antivirus logs/ exception reports				

SIGN-OFFS

Approved by Director Corporate Services:		**Signature:**		**Date:**	
Were there any Security Incidents? (Yes/No). **If yes, provide details and Incident No. and resolution**					

ANTIVIRUS MANAGEMENT POLICY

TABLE OF CONTENTS

1. OVERVIEW

This Policy establishes certain requirements which must be met by all computers connected to the AbaQulusi Municipality network to provide the AbaQulusi Municipality with a trusted and secure network infrastructure to support the effective delivery of IT resources and mechanisms to help the organisation realise its goals and objectives in maintaining a secure IT environment. It attempts to set standards in terms of antivirus software management.

2. PURPOSE

The purpose of this policy is to:

- To create awareness across the municipality of the importance of installing antivirus software.
- To establish requirements which must be met by all computers connected to AbaQulusi Municipality network to ensure effective virus detection and prevention.
- To provide a secure network environment for AbaQulusi Municipality automated applications, staff, business partners and contractors.
- To provide a resilient set of IT resources that maintains acceptable and agreed levels of confidentiality, integrity and availability.
- To ensure that all computer devices connected to the AbaQulusi Municipality network have proper virus-protection software with current virus-definition libraries.

3. SCOPE

This policy applies to all computers used on the AbaQulusi Municipality network that are PC-based or utilise PC-file directory sharing. This includes, but is not limited to; staff and third party desktop and laptop computers, file/ftp/tftp/ proxy servers, and any PC based equipment such as traffic generators. Computers that are not physically connected to the AbaQulusi Municipality network must also abide by this policy.

4. DEFINITIONS

Vulnerabilities - weaknesses in software that can be exploited by an entity to gain elevated privileges is authorised to have on a computer or system. Not all vulnerabilities have related patches. These situations require workarounds to attempt to mitigate “un-patched” vulnerabilities.

Threats - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

CERT - CERT is the Internet's official emergency team. CERT focuses on security breach and incidents, providing alerts and incident-handling and avoidance guidelines. CERT also conducts an ongoing public awareness campaign and engages in research aimed at improving security systems.

5. POLICY

5.1. All AbaQulusi Municipality PC-based computers must have AbaQulusi Municipality's standard, supported antivirus software installed and scheduled to run at regular intervals.

5.2. The antivirus solution will come with sufficient licenses for all user and devices attached to the network. The licenses will be renewed every two years and updates and patches shall be scheduled to run daily.

5.3. The antivirus software and the virus pattern files must be kept up-to-date.

5.4. Virus-infected computers must be removed from the network until they are verified as virus-free.

5.5. The ICT Manager is responsible for creating procedures that ensure antivirus software is run at regular intervals and computers are verified as virus-free.

5.6. Any activities with the intention to create and/or distribute malicious programs into AbaQulusi Municipality's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the End User Security Policy and ICT Security Policy.

5.7. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the ICT Department immediately by e-mailing or by calling the IT Helpdesk. The user must report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material, or simply log a call stating that you believe that a computer has an electronic viral infection.

5.8. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the ICT Department.

6. ANTIVIRUS SOFTWARE

6.1. Antivirus software installation and ICT responsibilities

6.1.1. ESET is the antivirus software that is used by the municipality. The antivirus software must be installed on all desktops, servers and laptops by ICT staff. The antivirus software must be active all the times.

6.1.2. The ICT Department is responsible for maintaining and updating this Antivirus Management Policy. Copies of this policy will be posted on the web site and the internal information portal. Check one of these locations regularly for updated information.

6.1.3. The ICT Department will keep the antivirus products it provides up-to-date in terms of both virus definitions and software version in use.

6.1.4. The ICT Department will invest adequate efforts to identify clients who did not attempt to update their virus definitions file for more than 3 months and will take appropriate remedial actions.

6.1.5. The ICT Department will apply any updates to the services it provides that are required to defend against threats from viruses.

6.1.6. The ICT Department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the ICT Department may be required to disconnect a suspected computer from the network or disconnect an entire segment of the network.

6.2. Antivirus software monitoring and updates

6.2.1. The server is updated daily for new virus definitions automatically and the system is configured to update at regular intervals on all client machines.

6.3. Review of antivirus logs

6.2.2. Antivirus logs/exception reports must be reviewed monthly by the ICT Manager. (Refer to the Monthly Activity Monitoring Checklist, Appendix B, in the Activity Monitoring Policy and Procedure).

7. Best Practices for Virus Prevention

7.1. Always run the standard antivirus software provided by the municipality.

7.2. Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

7.3. Never open files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

7.4. Be suspicious of e-mail messages containing links to unknown Websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

7.5. The municipality's email system scans all attachments for virus infections and blocks any trapped virus from being transmitted to client systems.

7.6. The desktop antivirus on the client machine scans all email attachments for virus infections. Also, and by default the e-mail client, Microsoft Outlook, blocks attachments with critical file extensions.

7.7. Users should not alter the default email client configuration to override the security setup and send/receive banned extensions. A workaround to send/receive such business critical files is to compress the file using a file compression utility.

7.8. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7.9. Avoid direct disk sharing with read/write access. Always scan any removable media for viruses before using it.

7.10. If instructed to delete email messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

7.11. Regularly update virus protection on personally-owned computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

8. End User Responsibilities

8.1. Users must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.

8.2. Users departments that allow employees to use personally-owned computers for business purposes, if applicable, must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

8.3. All employees are responsible for taking reasonable measures to protect against virus infection.

8.4. Employees must not attempt to either alter or disable antivirus software installed on any computer attached to the municipal network without the express consent of the ICT Department.

9. Enforcement

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

CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

TABLE OF CONTENTS

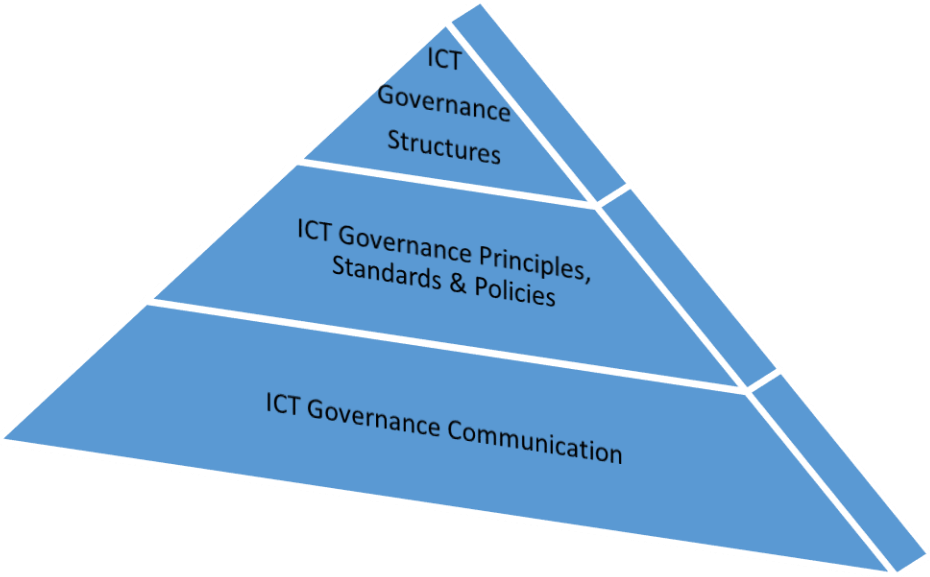
10. INTRODUCTION

Corporate governance consists of a governance system that depicts the way in which the municipality will be managed and controlled. It defines the relationships between stakeholders and the strategic goals of the municipality. Corporate governance is concerned with individual accountability and responsibilities within the municipality and is a vehicle through which value is created.

ICT Governance is defined as a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. ICT Governance can be further defined as the process by which decisions are made around IT investments and incorporate how decisions are made, who makes decisions, who is held accountable and how the results of the decisions are measured and monitored.

11. ICT GOVERNANCE FRAMEWORK

The figure below demonstrates AbaQulusi Municipality's ICT Governance Framework diagrammatically. Each of the components of the ICT Governance Framework is discussed in detail in the following sections.



12. ICT GOVERNANCE STRUCTURES

This section of the Governance of ICT Framework clearly defines who makes decisions, what structural organisations (e.g. ICT Steering Committee) will be created, who will take part in these organisations and what responsibilities they will assume.

6.4. ICT GOVERNANCE STRUCTURES AND DECISIONS

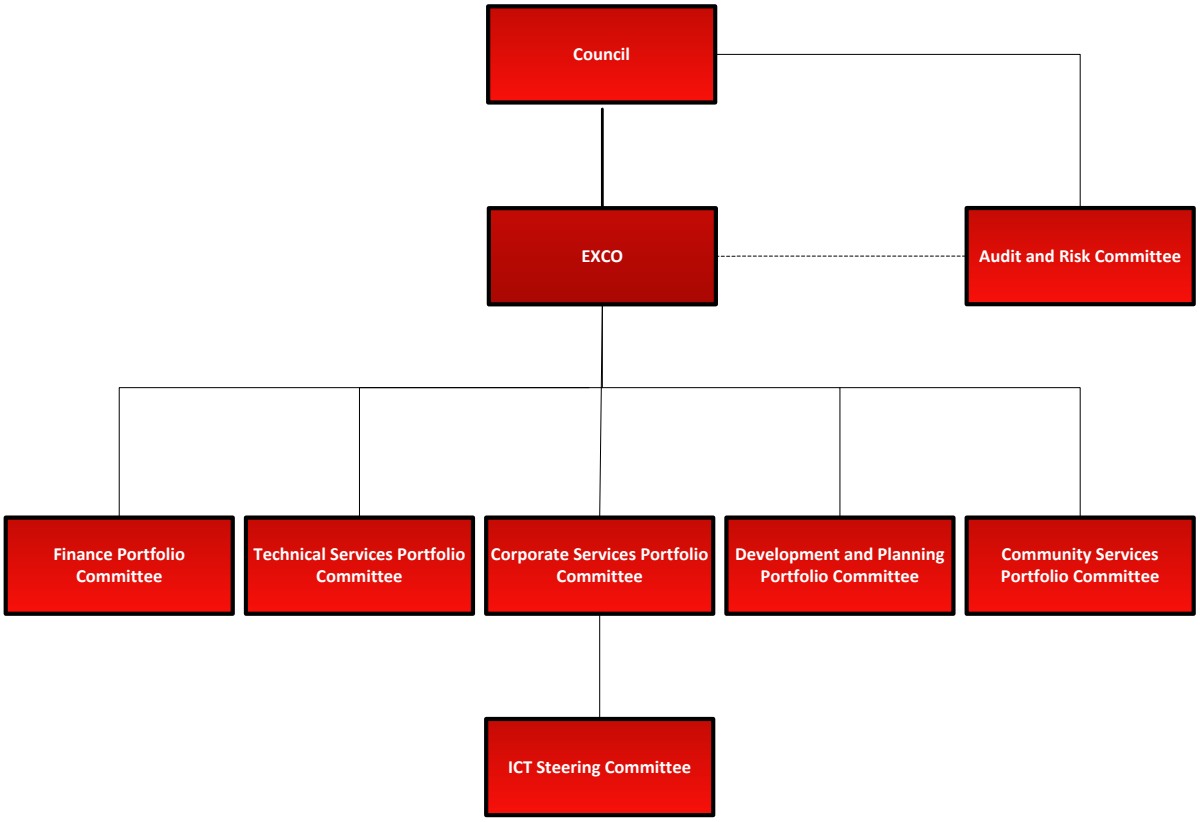
Structural organisations for ICT governance establishes the strategic, operational, and technical decision-making process required to ensure ICT enables AbaQulusi Municipality to excel in its mission. The objective is to establish a decision making body or committee, membership of the committee and the responsibilities of the committee.

The key decision making body for ICT decisions in AbaQulusi Municipality will be the ICT Steering Committee.

The ICT Steering Committee must take responsibility for making decisions with regard to the following IT decision categories:

a. ICT Governance, Risk and Compliance;
b. ICT Strategy;
c. Application Management;
d. Information;
e. Business and ICT Architecture;
f. ICT Investments and Projects;
g. ICT Sourcing;
h. ICT Security;
i. ICT Operations; and
j. General ICT Management and Administration.

The ICT Steering Committee will report ICT related information to the Corporate Services Portfolio Committee. The relationship between governance structures at AbaQulusi Municipality is illustrated on the diagram overleaf.


Council
EXCO
Audit and Risk Committee
Finance Portfolio Committee
Technical Services Portfolio Committee
Corporate Services Portfolio Committee
Development and Planning Portfolio Committee
Community Services Portfolio Committee
ICT Steering Committee

6.5. ROLES AND RESPONSIBILITIES OF THE STRUCTURAL ORGANISATION

The objective of this section is to identify and define the responsibilities of the ICT Steering Committee.

For each specific decision, AbaQulusi Municipality must consider the following:

a. The frequency of the decision (ad-hoc, annually);
b. The information required to make the decision;
c. Prerequisites for the decision to be made;
d. Impacts on other decision domains; and
e. Specific limitations on the scope of decisions.

When developing the decision model for each decision category, the type of involvement that is required from each stakeholder must be documented. The various roles that a stakeholder could have when participating in decision making are as follows:

a. Responsible for a decision: The stakeholder making the decision to achieve the deliverable.
b. Accountable for a decision: The stakeholder ultimately answerable for the decision that has been made and the one who delegates the work to those responsible.
c. Consulted for a decision: Stakeholders whose opinions are sought when making a decision.
d. Informed about a decision: Stakeholders who are kept up-to-date on progress or on decisions taken.

AbaQulusi Municipality stakeholders involved in the IT decision model are as follows:

a. EXCO;
b. Municipal Manager;
c. Audit and Risk Committee;
d. ICT Steering Committee;
e. Department Heads;
f. Director Corporate Services; and
g. ICT Manager.

The decision model adopted by AbaQulusi Municipality is depicted in below.

IT Decision Category	Decision Making Committee	Responsibility					
		Municipal Manager	Director Corporate Services	ICT Manager	Department Heads	EXCO	Audit and Risk Committee
ICT Governance, Risk and Compliance	ICT Steering Committee	A	R	R	I	I	I/C
ICT Strategy	ICT Steering Committee	A	R	R	I/C	C	I
Application Management	ICT Steering Committee	A	A	R	I/C	I	I
Information	ICT Steering Committee	A	C	R	I/C	I	I
Business and ICT Architecture	ICT Steering Committee	A	C	R	C	C	I
ICT Investments and Projects	ICT Steering Committee	A	R	R/C	I/C	C	I
ICT Sourcing	ICT Steering Committee	A	C	R	I	I	I
ICT Security	ICT Steering Committee	A	C	R	I	I	C
ICT Operations	ICT Steering Committee	A	C	R	I	I	I
General ICT Management and Administration	ICT Steering Committee	A	C	R	I	I	I

Key:

R	Responsible
A	Accountable
C	Consulted
I	Informed

13. BUSINESS AND ICT ALIGNMENT PLANNING

AbaQulusi Municipality will develop an ICT Strategy that will ensure that there is alignment between ICT and the business needs of the municipality. The ICT Strategy document will be reviewed on an annual basis and as part of this process the municipality's IDP as well as the views of senior management will be obtained and used to drive the strategic initiatives in the ICT Strategy.

14. ICT GOVERNANCE PRINCIPLES, STANDARDS AND POLICIES

PRINCIPLES

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organisation sets about fulfilling its mission.

Below are the guiding Corporate Governance of ICT Principles that have been adopted by AbaQulusi Municipality. These principles are recommended based on the principles described in the DPSA Public Service Corporate Governance of ICT Policy Framework (DPSA, 2012).

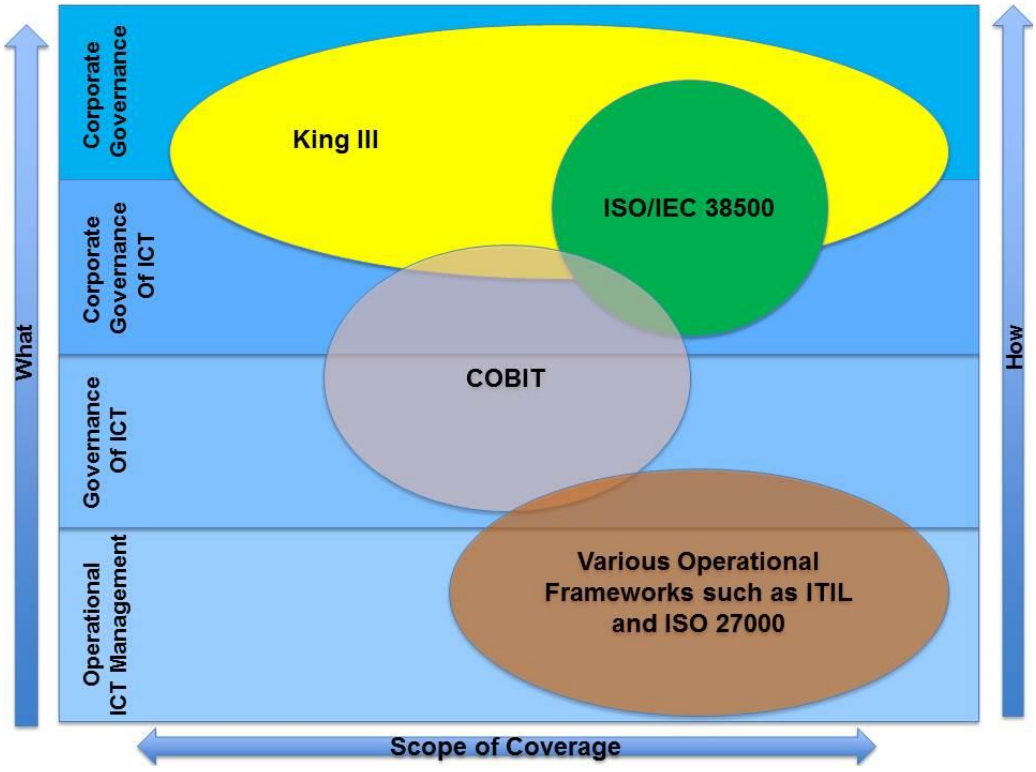
No.	Principle	Description
1	The corporate governance of ICT must enable the municipality's political mandate.	The municipal manager is responsible to ensure that corporate governance of ICT assists AbaQulusi Municipality in achieving its political mandate.
2	The corporate governance of ICT must enable the municipality's strategic mandate.	The municipal manager is responsible to ensure that corporate governance of ICT achieves the municipality's strategic goals.
3	ICT should be aligned with the strategic goals of the municipality.	The municipal manager must ensure that ICT is aligned with AbaQulusi Municipality's strategic goals and that business needs influence the current and future capabilities of ICT. It must ensure that ICT is fit for purpose at the correct service levels and quality for current and future business needs.
4	The municipal manager is responsible for the corporate governance of ICT.	The municipal manager must create an enabling environment in respect of the corporate governance of ICT within the applicable judiciary and information security context.
5	The municipal manager should monitor and evaluate significant ICT investment.	The municipal manager is responsible to monitor and evaluate major ICT investment and must ensure that ICT investment is made for valid business enabling reasons. The municipal manager must further monitor and manage the benefits, opportunities, costs and risks resulting from these investments whilst ensuring that information assets are adequately managed.
6	The municipal manager should ensure that ICT Risk is managed	The municipal manager is responsible to ensure that ICT risks are managed as well as

No.	Principle	Description
	and that the ICT function is audited.	the ICT function is audited.
7	The municipal manager should ensure that ICT service delivery is sensitive to organisational behaviour/culture.	The municipal manager must ensure that the use of ICT demonstrates the understanding of and respect for organisational behaviour/culture.

STANDARDS

A standard is defined as a document established by consensus and approved by a recognised body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

The figure below depicts the different layers of governance and the interrelationship between the different Frameworks and Standards as recommended by DPSA. All of the frameworks reflected in the figure are generally accepted frameworks. King III is the corporate governance standard adopted by most entities in South Africa and the other standards like ISO, ITIL and COBIT are internationally recognised frameworks and standards operating at different levels within the ICT Governance Framework.



Source: DPSA – Public Service Corporate Governance of Information and Communication Technology Policy Framework (2012).

The figure above reflects the frameworks, standards and codes that have been used to develop the ICT Governance Framework. This is in-line with DPSA guidelines and all of the standards, frameworks and codes reflected in the figure above are internationally recognised or generally accepted standards.

The table below provides a general description of each standard or framework.

Framework/Standard	Description	Application
King III	King III Code is a Code of Good Governance emphasising corporate leadership, business sustainability and corporate citizenship. The King III Code is the most commonly accepted corporate governance framework in South Africa and is also valid for the Public Service.	Guides corporate governance practices at an entity level but has a specific chapter dealing with IT. DPSA have adopted King III IT recommendations and principles to guide IT governance in public entities. As such, chapter 5 of King III has been used as a reference when developing this document and the ICT Charter.
ISO/IEC 38500	ISO/IEC 38500 is an international standard for the corporate governance of ICT, which provides a framework of principles for the executive authority and management to govern and manage ICT.	This Governance of ICT Framework Policy is based on this standard.
COBIT	COBIT is an internationally accepted process framework for the implementation of the governance of ICT. COBIT fully supports the principles of the King III Code and the ISO 38500 standard on the corporate governance of ICT.	This will be used to guide the development of policies that are required by the municipality as per DPSA guidelines.
ISO/IEC 27002	ISO/IEC 27002 is a code of practice for information security management. It can be used by any organisation that needs to establish a comprehensive information security management program or improve its current information security practices. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).	This standard will be used to guide information security management within the municipality.

POLICIES

A policy sets direction and expectations on a subject. It is approved at the highest level of the organisation and is designed to remain in effect regardless of changes in people, technology or the mission of the organisation. The need for policies is driven by the business objectives, resource requirements, organisational risks, rules and legislation and the maturity level of the organisation. It also provides guidance for standards, processes and procedures, controls and structures. IT Policies are concise, high-level and independent of a given technology.

Policies and Frameworks are defined in the DPSA's "Public Service Corporate Governance of ICT Policy Framework" document, which states that the following should be implemented by March 2014:

a. Corporate Governance of ICT Policy Framework

b. Governance of ICT Framework
c. Governance of ICT Charter
d. Risk Management Policy
e. Internal Audit Plan
f. ICT Management Framework
g. ICT Portfolio Management Framework
h. ICT Security Policy
i. ICT Continuity Plan

15. ICT GOVERNANCE COMMUNICATION

The ICT Governance Framework must also clearly define the communication mechanism that will be used to communicate ICT Management decisions to relevant stakeholders within the municipality.

a) Communication of ICT Governance policies and decisions must be communicated to the AbaQulusi Municipality business. The following mechanisms may be utilised:

    i. Publishing information on the intranet; and
    ii. Newsletters.

b) Certain key IT decisions must be documented in ICT policies and procedures and communicated to the stakeholders as and when these updates occur.

DISASTER RECOVERY PLAN

TABLE OF CONTENTS

1. INTRODUCTION

The AbaQulusi Municipality's IT systems and networks provide core services and functionality that each business unit within the municipality is dependent upon.

In recognition of these dependencies, it is of utmost importance that AbaQulusi Municipality be prepared to respond to a disaster in an orderly, timely and efficient manner.

This document describes the Recovery Plan which will be used in the event of a disaster that might affect the AbaQulusi Municipality's operation and services. It includes a summary of the current services, identifies the services critical to municipal operations and dictates how these services will be reconstituted following a disaster.

A current version of this plan, the plan's appendices and any other referenced policies and procedures must be kept in a secure offsite location to ensure that the plan is available in the event of a disaster.

2. SCOPE OF THIS PLAN

This plan provides AbaQulusi Municipality with the ability to address two areas:

2.1. It enables the systems administrator to restore AbaQulusi Municipality's core information systems in the event of a disaster.

2.2. It identifies areas of substantial risk and exposure to disaster and assist in reducing these risks.

3. DISASTER SCENARIOS

This plan focuses on recovering from a disaster at the AbaQulusi Municipality head office, Corner of Mark & High Street, Vryheid. This building is deemed most critical. This is where core IT systems are housed. Technical Services, cnr. Of Mason and Mark street will be used as a Disaster Recovery site.

4. CURRENT PRACTICES AND PROCEDURES

An understanding of fundamental municipal practices is the key to recovering the municipality's operations, the key activities include:

4.1. DATA BACKUP AND RESTORATION

Backups are performed in accordance with the Municipalities Data Backup and Restoration policy and procedures. These require that all business critical systems are adequately backed up and tested to ensure that key systems and information can be recovered.

4.2. APPLICATION RESTORATIONS

The different systems restoration procedures will define how each system/application will be restored. Where necessary, the expertise of the system Vendor or Service Provider will be utilised.

4.3. CRITICAL SYSTEMS

The following systems are designated as critical systems and are critical to the continued running of the municipality:

System	Processes relying on	Operating System	Database	IP Address

	System			
MunAdmin	Electronic Document Management	Windows Server 2008 R2	Nexus	
MunSoft	Financial System (ERP)	LINUX	Oracle	
Payday	Payroll HR	LINUX	MySQL	
TCS	Traffic - Fines, Court rolls	Windows XP Pro	COBOL	
ESS	Leave	LINUX	MySQL	
Payday T&A	Time and Attendance	Windows 7 Pro	SQL	
Contour	Pre-paid Electricity		SQL	
Webmin	Firewall	LINUX		
ArcGIS	Town Planning, Spatial mapping	Windows 2000	Shape Files	
Caseware	Financial Reporting Tool			

4.4. DRP MANAGEMENT

4.4.1. The ICT Manager is the primary person responsible for ensuring Disaster Recovery Plans (DRP) are regularly reviewed, tested and maintained.

4.4.2. The ICT Manager is required to liaise with all DRP teams on a regular basis to ensure all changes within the municipality and their impact on Disaster Recovery have been considered.

4.4.3. The ICT Manager is also responsible for ensuring that all staff members within the municipality are provided with the necessary awareness and training.

4.4.4. The ICT Manager will be responsible for ensuring that the Disaster Recovery Plan is kept in a safe and secure place and he is in possession of the latest version of the plan.

5. NOTIFICATION AND ACTIVATION

5.1. Upon discovery of a disaster, the Municipal Manager, Director: Corporate Services, Chief Financial Officer and ICT Manager must be notified immediately.

5.2. The person who has authority to declare a disaster is the Municipal Manager in consultation with the Director Corporate Services and ICT Manager.

5.3. The ICT Manager will then perform an assessment of the municipality's IT Systems, based upon which the Municipal Manager will determine whether it is appropriate for the Disaster Recovery Plan to activated and invoked.

5.4. Should the Municipal Manager not be available the responsibility will then sit with the Director Corporate Services.

5.5. Once the plan has been formally invoked, the following procedures must be followed.

6. RECOVERY PROCESS

The recovery process consists of two phases:

a. An initial phase where notifications are made, the staff assembled, information gathered and an action plan developed.
b. The recovery phase where resources are acquired, data recalled and services are restored as much as possible.
c. If there is a disaster of any kind, it must only take a maximum of five days to recover and have all users online for critical systems.

PHASE 1 – ASSESSMENT AND PLANNING

6.1.1. NOTIFY AND ASSEMBLE THE RECOVERY STAFF

6.1.1.1. All recovery staff should be notified as soon as the decision to invoke the Disaster Recovery Plan has been made.

6.1.1.2. The recovery team, comprising of the key system users, application vendors (where applicable) and the ICT Manager, should then assemble at the Disaster Recovery Site.

6.1.1.3. Refer to the Recovery Staff Details for names and contact details of the Recovery Team.

6.1.1.4. Once the recovery team has been assembled, they should go through the Disaster Recovery Plan to assign roles and responsibilities and ensure that everyone knows and understands their specific roles and tasks.

6.1.2. PERFORM PRIMARY SITE PROCEDURES

6.1.2.1. It is the Recovery Team's responsibility to conduct a site survey of affected area to assess the nature and extent of any damage.

6.1.2.2. The Recovery Team must take stock of any salvageable or usable equipment and note what equipment will need to be replaced.

6.1.2.3. The Recovery Team must also secure the primary site so as to ensure that there is no unauthorised access to what may remain of the municipality's IT systems and to prevent any further damage.

6.1.3. INFORM VENDORS AND SERVICE PROVIDERS

6.1.3.1. Once the nature and extent of the disaster has been determined, the municipality's vendors and service providers should be notified and informed that the municipality has invoked its Disaster Recovery Plan and what assistance or equipment they should provide.

6.1.4. ESTABLISH COMMUNICATION PLAN

6.1.4.1. A communication plan will need to be implemented. The communication plan will ensure that:

6.1.4.2. All municipal staff and contractors impacted by the Disaster are informed and instructed on what they should do, i.e. stay at home, report to DR site etc;

6.1.4.3. EXCO is kept up-to-date on a regular basis with status updates and estimated timelines;

6.1.4.4. All relevant municipal Suppliers, Vendors, Service Providers or Customers should be informed and kept updated where appropriate;

6.1.4.5. Communication with the relevant authorities, Police, Fire Department etc, is centralised and the responsibility given to a specific individual/s who can then relay any messages with the Disaster Recovery team.

6.1.4.6. Any and all communication with the Media, if required or requested, should be directed to a specific, authorised individual who can speak on the municipality's behalf.

PHASE 2 - RECOVERY

6.1.5. SYSTEM RECOVERY PRIORITY LIST

6.1.5.1.1. The priority of the municipality's systems and the order in which they should be recovered are:

Priority	System
1	MunAdmin
2	MunSoft
3	Payday
4	TCS
5	ESS
6	Payday T&A
7	Contour
8	Webmin
9	ArcGIS
10	Caseware

6.2.1.1.2. Vendor and/or Service Provider expertise will be utilised during the recovery procedure if required to ensure that the systems are effectively restored in as short a time as possible. Application software, Operating System disks, drivers and other critical software must be maintained at the recovery site.

6.2.2. EQUIPMENT LIST

6.2.2.1.1. The following equipment is required to re-establish the priority service to a basic nominal level of service. It is not intended to duplicate the original performance, but rather to provide a minimally acceptable level. This equipment will be obtained from service providers and from the open market. This equipment will be set up at the Technical Services building which will be used as a Disaster Recovery Centre as a precautionary measure in case a disaster strikes.

6.2.2.1.1.1. Desktop Computer;

6.2.2.1.1.2. Linux server;

6.2.2.1.1.3. Windows server;

6.2.2.1.1.4. Printers;

6.2.2.1.1.5. Backup media; and

6.2.2.1.1.6. Network Disaster Recovery Server.

6.2.2.1.1.7. Switches

6.2.3. RE-ESTABLISHMENT OF NORMAL OPERATIONS

6.2.3.1. As part of the recovery process consideration must also be given to restoring the municipality's systems to a normal state of operations. Whilst priority will be given to restoring the minimal operating requirements of the

municipality, once this is achieved focus must shift to re-establishing the normal state of operations.

6.2.3.2. Steps required to be taken will depend on the nature and extent of the disaster but may, at a minimum, include the following:

6.2.3.2.1. Acquisition of equipment to permanently replace destroyed or damaged equipment. This equipment should be of a suitable specification to enable pre-disaster performance to be achieved;

6.2.3.2.2. Identification of a suitable server room if the original one is no longer suitable;

6.2.3.2.3. Implementation of a cutover plan to transfer all data from DR systems back onto Production systems.

6.2.4. PROCEDURE FOR THE RETRIEVAL OF BACKUP MEDIA

6.2.4.1. The type of backup media used for are backed up remotely by the respective Service Providers and data backup drives.

6.2.4.2. If on-site backups are available, restore using the most recent backup CD/ Tapes.

6.2.4.3. If on-site backups are destroyed, retrieve the latest backup from the off-site location and restore.

6.2.5. POST RECOVERY REVIEW

6.2.5.1. Within a month of normal operations having been restored a post recovery review must be performed by the Recovery Team.

6.2.5.2. This review must identify and document any and all weaknesses or issues identified during the recovery process.

6.2.5.3. The remediating actions taken must be documented and the Disaster Recovery Plan updated accordingly.

6.2.5.4. The review should also identify areas where efficiencies could be made and these should be included in the next test of the Disaster Recovery Plan.

7. PLAN MAINTENANCE AND TESTING

7.1. This Disaster recovery plan must be tested, at a minimum, on an annual basis.

7.2. The testing should simulate a Disaster and all necessary recovery steps must be performed as per the documented plan.

7.3. The testing must be documented and all documentation must be retained.

7.4. Any weaknesses or issues identified during testing should be remediated and the Disaster Recovery Plan updated accordingly.

8. APPENDICES

8.1. RECOVERY STAFF DETAILS

Upon activation of the municipality's Disaster Recovery Plan, the following individuals must be contacted to form part of the recovery team:

Name	Job Title	Contact Details
David Johnson	ICT Manager	072 640 1030
Werner Leach	Senior Engineer	083 535 8099
IT Technician	Junior Technician	

8.2. VENDORS AND SERVICE PROVIDERS

The following are the municipality's key Vendors and Service Providers:

Service Provider	System/Service	Contact Person	Contact Number
Munsoft	Munsoft	Martin/Yvette	(011) 215 8000
MunComp	MunAdmin	Andre	084 585 4390
TCS	TCS	Call Center	
Proxy Servers	AQM/DCData	Tech support Center	033 344 6100
Email Server	AQM/DCData	Tech support Center	033 344 6100

8.3. EMERGENCY SERVICES

The following are emergency services details:

Emergency Services	Contact Number
Police	10111
Fire Department	034 328 4700 / 034 982 2948
Ambulance	034 983 2162
Hospital	

8.4. UTILITIES SERVICES

The following are Utilities services details:

Utilities Services	Contact Number
Electrical	034 982 2133
Sewer	034 982 2133
Water	034 982 2133
Sanitation	034 982 2133

END USER SECURITY POLICY

Table of Contents

1. INTRODUCTION

This policy is intended to define the requirements for managing access to AbaQulusi Municipality, Information Communication Technology (ICT) resources.

The Policy covers all information resources that are owned by AbaQulusi Municipality or used by AbaQulusi Municipality under license or contract. This includes information recorded on all types of analogue and digital media, computer hardware and software, paper, computer networks, and telephone systems.

2. User Confidentiality & Privacy

2.1. Compliance with legal requirements

2.1.1. AbaQulusi Municipality will identify, document and maintain relevant statutory and regulatory requirements that may have an impact on the way security controls are deployed. AbaQulusi Municipality will therefore deploy security controls accordingly.

2.2. Sensitive classifications

2.2.1. Information (incl. data, applications and certain processes) will be classified based on its nature and the sensitivity of it.

2.2.2. Data shall be classified as either: Confidential, Sensitive or Public.

2.2.3. Confidential: Sensitive data that must be protected from unauthorised disclosure or public release based on local or governmental law (e.g. the Promotion of Access to Information Act, No. 2 of 2000) and other constitutional, statutory, judicial and legal agreements.
Examples of "Confidential" data may include but are not limited to:

- 2.2.3.1. Personally Identifiable Information, such as a name in combination with Identification Number (ID) and/or financial account numbers
- 2.2.3.2. Employee records
- 2.2.3.3. Intellectual Property, such as copyrights, patents and trade secrets

2.2.4. Sensitive: Sensitive data that may be subject to disclosure or release under the Promotion of Access to Information Act, No. 2 of 2000, but requires additional levels of protection. Examples of "Sensitive" data may include but are not limited to:

- 2.2.4.1. Operational information
- 2.2.4.2. Personnel records
- 2.2.4.3. Information security procedures
- 2.2.4.4. Research
- 2.2.4.5. Internal communications

2.2.5. Public: Information intended or required for public release as described in the Promotion of Access to Information Act, No. 2 of 2000. However, any data owned or under the control of the South African Government must comply with the national classification authority and national protection requirements.

2.3. Restricted information

2.3.1. Restricted information should not be collected and stored unless absolutely necessary.

2.3.2. Restricted information should not be stored on portable devices. If it is necessary to store restricted information on portable devices, ensure the appropriate protection measures, such as encryption, are in place before installing restricted data on the device.

2.3.3. Access to restricted information should be adequately secured and authorised only as needed to perform assigned duties.

2.3.4. Restricted data should be deleted when there is no longer a business need for its retention.

2.3.5. When restricted information is distributed, include a notification that the data is restricted and that it requires specific security protection.

3. User Monitoring

3.1. Communication and Network Activities

3.1.1. AbaQulusi Municipality's communication systems will primarily be used for business purposes.

3.1.2. All messages and information, which are sent through the internal computer and communications systems, will be deemed the property of AbaQulusi Municipality.

3.1.3. AbaQulusi Municipality reserves the right to monitor, access, retrieve, read, and/or disclose employee communications at any time when:

3.1.4.1. A legitimate business need for such action exists;
3.1.4.2. The involved employee is unavailable and timing is critical to a business activity, provided the employee has given prior consent for such action;
3.1.4.3. There is reasonable cause to suspect criminal activity or material violation of the municipality's policies; and
3.1.4.4. Monitoring is required by law, regulation, or a third-party agreement.

4. Email

4.1.1. AbaQulusi Municipality reserves the right to, and shall monitor all incoming and outgoing emails.

4.1.2. Municipality email systems must primarily be used for business purposes.

4.1.3. All e-mail messages are required to have the following standard signature and disclaimer attached to all outgoing messages:

Kind Regards,
Name & Surname | Position Held
AbaQulusi Municipality | Cnr. Mark & High Street | Vryheid | 3100 |
Mobile: +27 00 000 0000 | Fax: + 27 00 000 0000 |Tel: +27 00 000 0000 Ext. 0000
email@abaqulusi.gov.za | www.abaqulusi.gov.za

"The information contained in this communication is confidential and may be legally privileged. It is intended solely for the use of the individual or entity to whom it is addressed and others authorized to receive it. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking action in reliance of the contents of this information is strictly prohibited and may be unlawful. Municipality is neither liable for the proper, complete transmission of the information contained in this communication nor any delay in its receipt."

5. Email Usage

5.1. CONDITIONS FOR BUSINESS USE

The use of email for AbaQulusi Municipality business use must be within, but not limited to the following conditions:

5.1.1. Employees should not allow family members or other non-employees to access and use the AbaQulusi Municipality email system.

5.1.2. Employees should not allow other employees to access and use their email accounts unless authorised by the ICT Manager.

5.1.3. Personal email accounts with Internet Service providers or third parties should not be used from AbaQulusi Municipality computers.

5.1.4. Disciplinary action may occur after actions including or similar to those stated below of AbaQulusi Municipality email facilities has occurred:

5.1.4.1. Copying of electronic files, information and documents without permission; and

5.1.4.2. Transmission of AbaQulusi Municipality files, documents or any other electronic data/information outside of AbaQulusi Municipality or inside AbaQulusi Municipality to unauthorised personnel.

6. Personal Use

AbaQulusi Municipality is aware that email may be used for limited personal purposes. However, all employees must recognise that the email facility is primarily a business tool and that all personal communication should be kept to a minimum. Employees should demonstrate a sense of responsibility and to ensure that they are not perceived as abusing this privilege.

Personal use of email facilities is a privilege and not a right and this privilege can be revoked at any stage at the sole discretion of ICT Management.

6.1. CONSTRAINTS ON PERSONAL USE

Users may use email for coincidental personal purposes on condition that:

6.1.1. It does not consume significant amounts of the user's workday.

6.1.2. It does not consume substantial amounts of AbaQulusi Municipality's bandwidth in such a way that it negatively impacts upon the email system, either directly or indirectly.

6.1.3. Bandwidth could be impacted by distribution of the following:

6.1.3.1. Large email messages. Users should consider using compression utilities such as Zip before sending large email messages;

6.1.3.2. Attachment types such as JPEG, JPG, AVI, etc; or

6.1.3.3. Chain letters, jokes, bitmaps, etc.

6.1.3.4. Downloading of email content such as executable programmes or other such files unless this action is necessary for the business purposes and has the approval of the ICT Manager.

6.1.4. It does not expose AbaQulusi Municipality to a noticeable increase in costs.

6.1.5. It does not expose AbaQulusi Municipality to reputational or financial risks.

6.2. PRIVACY OF EMAIL (ACCESS TO EMPLOYEES' EMAIL USAGE)

6.2.1. As AbaQulusi Municipality allows the incidental and infrequent personal use of email, users must be aware of the restrictions placed on the privacy of email.

6.2.1.1. The municipality respects the individual privacy of its employees, however, employee privacy does not extend to the employee's work-related conduct; and

6.2.1.2. The municipality reserves the right to access and monitor all emails on the municipality's email system. Employees should not assume that emails are totally private and should consider encrypting highly confidential data when sending this in an email.

6.2.2. The purpose of the email system is to facilitate business communications. Although each employee has an individual password to access this system, all data and contents of emails remain the property of the municipality and can be accessed by management for any of the following cases below:

6.2.2.1. A legitimate business need for such action exists;

6.2.2.2. The involved employee is unavailable and timing is critical to a business activity, provided the employee has given prior consent for such action;

6.2.2.3. There is reasonable cause to suspect criminal activity or material violation of the municipality's policies;

6.2.2.4. Monitoring is required by law, regulation, or a third-party agreement.

6.2.3. Employees should be aware that the following guidelines may affect their privacy in the workplace:

6.2.3.1. AbaQulusi Municipality routinely monitors usage patterns for its email communications. The reasons for this monitoring include but are not limited to cost analysis/allocation, the management of the municipality's gateway to the email system and to detect security violations.

6.2.3.2. Where required, AbaQulusi Municipality will disclose information obtained through such examinations to appropriate third parties, including law enforcement agencies.

6.2.3.3. All information created, sent, or retrieved through the email system is the property of AbaQulusi Municipality.

6.2.3.4. Employees must respect the confidentiality of other individual's emails and may not attempt to read, "hack" into other systems or other people's logins, or "crack" passwords.

6.2.3.5. Employees may not breach computer or network security measures, monitor electronic files or communications of other employees or third parties except

by explicit direction from the ICT Manager with consultation from Executive Management.

6.2.3.6. No emails may be sent which attempt to hide the identity of the sender, or represent the sender as someone else or from another municipality.

6.2.3.7. Anyone obtaining electronic access to the material of other companies or individuals must respect all copyrights and may not copy, retrieve, modify or forward copyrighted material except as permitted by the copyright owner or a single copy for reference use only.

6.3. EXPRESSLY PROHIBITED USE

Note that progressive discipline will be applied for transgressions of the above, commencing with counseling. However, there are certain transgressions which are completely unacceptable to AbaQulusi Municipality and are expressly forbidden. These are scheduled below and failure to comply with these rules will result in disciplinary action which could result in dismissal even for the first offence:

6.3.1. Threats;
6.3.2. Pornographic or sexually explicit material;
6.3.3. Material containing derogatory racial, gender, religious or hate-oriented comments;
6.3.4. Libelous remarks about products or other companies,
6.3.5. Defamatory remarks, including defamation of character;
6.3.6. Discriminatory language or remarks that would constitute harassment of any type.
6.3.7. Any other comments that offensively addresses someone's age, political beliefs, national origin, or disability.
6.3.8. The forwarding of chain emails is prohibited and any chain mail received is to be deleted. Chain mail is defined as an email containing a message which attempts to induce the recipient to forward the email on to as many recipients as possible.

6.4. UNSOLICITED EMAIL

6.4.1. When an employee receives unwanted email(s) e.g. junk mail or spam, the employee must refrain from responding directly to the sender. Instead, the employee should delete the email.

6.5. IMPERSONATION

6.5.1. Impersonation of another user when using email is prohibited within AbaQulusi Municipality.

6.5.2. Users should not allow others to use their email accounts.

6.6. RETENTION OF EMAIL MESSAGES

6.6.1. Email shall be retained for periods that would normally apply to written or facsimiled transactions.

7. Internet

7.1. GENERAL

7.1.1. All network connections permitting connectivity to the Internet will be monitored 24 hours per day, 7 days per week.

7.1.2. AbaQulusi Municipality internet systems must primarily be used for business purposes.

7.1.3. AbaQulusi Municipality reserves the right to monitor and restrict internet traffic through its access points in order to effectively manage the performance of and to secure its investment in services and networks. All usage will be monitored, filtered and restricted where appropriate.

7.2. USAGE

7.2.1. AbaQulusi Municipality will implement as many of the following internet controls as possible:

7.2.1.1. Monitoring and filtering content accessed via web browsing and any other Internet services for appropriate use

7.2.1.2. Detecting malicious content

7.2.1.3. Detecting unauthorised disclosure of municipal information

7.2.1.4. Allowing only authorised, authenticated users access to web resources

7.2.1.5. Logging access

7.2.1.6. Detecting and blocking unapproved applications and protocols tunnelling through open, permitted ports

7.2.2. AbaQulusi Municipality reserves the right to intercept and quarantine networking traffic and computing resources, such as Internet mail and other Internet services, which may pose a threat to AbaQulusi Municipality.

7.2.3. Internet access is provided to assist in the accomplishment of the AbaQulusi Municipality's business goals. Limited personal use of the Internet is permitted within strict guidelines, which, is controlled by content checking software to limit sites visited.

7.2.4. Use of the Internet for obtaining or distributing pornographic or sexually oriented materials is strictly prohibited.

7.2.5. Users must ensure that precautions are taken to protect AbaQulusi Municipality's networking and computing resources when obtaining software, files, and data from external sources. The introduction and use of software, files, and data containing malicious software or viruses into AbaQulusi Municipality's computing environment has the potential for serious disruption of the municipalities business. All users have the

responsibility of ensuring that all software, files, and data entering the municipalities computing environment are properly scanned for potential threats by utilising the antivirus software.

7.2.6. Using AbaQulusi Municipality's networking and computing resources to make or attempt unauthorised entry to any network or computer accessible via the Internet, is strictly prohibited.

7.3. PRIVATE USE

7.3.1. An employee may use the municipality's internet browsing system for incidental personal purposes provided that it does not:

7.3.1.1. Directly or indirectly disrupt municipality's internet system;

7.3.1.2. Expose the municipality to a marked increase in cost; or

7.3.1.3. Interfere with the user's daily work activities.

7.4. DOWNLOADING

7.4.1. Activities that cause a sustained high volume of network traffic such as downloading are to be avoided unless there is a strong business requirement.

7.4.2. Users may not download, install or copy any software specifically designed to circumvent any existing security mechanism or features.

7.4.3. Downloading of information or software through Instant Messaging or Chat mechanisms is prohibited as these could bypass the municipality's Internet safeguards.

8. Software Installations

8.1.1. Only business related software is allowed to be installed on any computing device.

8.1.2. Users requiring software to be installed on their computers must log a call and the request for software installation to be approved before it can be installed. Only the ICT department can install the software.

8.1.3. Under no circumstances should unlicensed software be installed on any AbaQulusi Municipality devices.

9. User Access

9.1. Password Controls

9.1.1. All employees, contractors and temporary staff that have access to AbaQulusi Municipality systems will be allocated a unique username and password.

9.1.2. Users carry the risk if passwords are shared and will be held responsible for all activities performed with their user accounts. Passwords may not be written down or stored electronically.

9.1.3. The use of another user's account and password is strictly forbidden.

9.1.4. Misrepresenting, obscuring, suppressing or replacing a user's identity on any IT system is strictly forbidden.

9.1.5. Users should not choose to "Remember Password" on any application.

9.1.6. The allocation of passwords must be strictly controlled through a formal management process.

9.1.7. When a password is initially assigned to a user, the password shall be a temporary one and the user shall be forced to change it immediately.

9.1.8. A procedure for providing users who have forgotten their password with a new password must be in place. The procedure(s) are detailed in AbaQulusi Municipality User Access Management Policy/Procedure.

9.2. Passwords must conform to the following:

9.2.1. Minimum length: 8 characters

9.2.2. Maximum age: 30 days

9.2.3. Composition: Alphanumeric. Special characters are optional

9.2.4. A password history of 24 generations should be maintained

9.2.5. Should not comprise any aspects of a date, family or municipality identifiers, telephone numbers, the user ID or other system identifiers or more than two consecutive identical characters

9.2.6. Words are not allowed as they appear in the dictionary. Dictionary words must be combined with alphanumeric characters.

9.2.7. Unmanned workstations must be locked and have a password protected screensaver enabled. The screensaver setting should be set to 5 minutes of inactivity.

9.2.8. User accounts will be locked automatically if the user enters the incorrect password on 3 consecutive occasions.

9.2.9. The account will remain locked until the ICT Manager unlocks it.

9.3. Access Provisioning

9.3.1. Access to IT systems or services must be authorised in accordance with AbaQulusi Municipality's User Account Management procedures.

9.3.2. The ICT Manager must ensure that all users with access to IT systems or services under their control have been formally authorised to have such access.

10. Physical Security and Care

10.1. Visitors

10.1.1. Visitors shall be supervised and their date and time of entry and departure recorded.

10.1.2. Visitors are only to be granted access for specific, authorised purposes and shall be issued with instructions on the security requirements and emergency procedures.

10.2. Restricted Areas

10.2.1. Only employees, temporary staff and contractors with a requirement to access AbaQulusi Municipality's Computer Room should have access. All access has to be applied for and approved by the ICT Manager.

11. Virus and Malicious Software

11.1. Awareness

11.1.1. Virus and malicious code attacks are a constant threat to the confidentiality, integrity and availability of IT resources. AbaQulusi Municipality has put in place controls to prevent, detect and eradicate such events. All staff, contractors and temporary staff should be aware of this threat.

11.2. Responsibility

11.2.1. Users need to take the necessary care and precaution in order to prevent viruses and malicious code from being released on to the AbaQulusi Municipality IT systems and network.

11.2.2. All employees are to ensure that their computers are enabled with the AbaQulusi Municipality approved virus protection software. To avoid the transmission of viruses, employees should first scan external devices, USBs, CD-ROM's etc for resident viruses prior to accessing the information.

11.2.3. Where an employee suspects that an e-mail message or an attachment, external storage device or CD-ROM may contain a virus s/he is required to scan the device, otherwise contact the ICT Helpdesk to have a call logged and attended to.

11.2.4. All external devices must be scanned for viruses and malicious software using the antivirus software provided by AbaQulusi Municipality. In the event that a virus or malicious software is detected the ICT Helpdesk and the ICT Manager must be notified. The device must not be connected to the AbaQulusi Municipality network until the virus or malicious software is removed.

12. Data Management, Device handling & Storage

12.1. Wi-Fi Usage

12.1.1. Wireless networks must be maintained at the same security levels as an un-trusted Internet connection and require the same safeguards, including encryption, logging and strong authentication to be in place before their use.

12.1.2. If Wi-Fi cards/devices are not being used, they should always be switched off.

12.1.3. In the event that a user would need to connect to the AbaQulusi Municipality's network a VPN connection must be used.

12.1.4. Users should always use a WPA2 or better encryption on wireless networks. When using a WEP network, users should not try and send/receive sensitive/confidential information as it is unsafe.

12.1.5. Users connecting to hotspots without WEP or WPA should only send or receive municipality information over a VPN connection. In addition the ICT department must load a personal firewall on their laptops. Users should try and avoid making use of unprotected hotspots unless absolutely necessary.

12.2. Encryption of laptops and external devices

12.2.1. All AbaQulusi Municipality's laptop users must ensure that the encryption software has been installed on their machines.

12.2.2. All external storage devices (memory cards, flash disks, external hard drives or any other form of device that can store electronic data) must be encrypted before AbaQulusi Municipality data is copied onto the device.

12.2.3. In the event that an external storage device or laptop is lost or stolen the ICT Manager must be contacted and notified immediately of the incident. A copy of the SAPS report must also be provided.

12.3. Use of personal computers, hardware and related DTP assets

12.3.1. Personal computers, hardware, software and related assets must be safeguarded against environmental hazards (dust, excessive heat, damp, lightning, etc) and unauthorised use at all times.

12.3.2. As with other AbaQulusi Municipality assets, no computer hardware or software may be removed from the AbaQulusi Municipality premises without authorisation.

12.3.3. Laptops and other moveable computer devices must be secured when the employee is away from his/her work area. While an employee is away on extended absence from the workplace, not making use of such devices, or on leave, these devices must be secured.

12.3.4. AbaQulusi Municipality's normal Supply Chain policies and procedures will be used when purchasing all computer hardware, software and peripheral devices.

12.3.5. All computer hardware and software problems must be reported to the ICT Helpdesk for resolution.

13. Appendices

Employee/Contractor Agreement

Appendix A

Employee/Contractor Agreement

I have received a copy of AbaQulusi Municipality's End User Security Policy; I recognise and understand that AbaQulusi Municipality e-mail, Internet and computer systems are to be used for conducting AbaQulusi Municipality business only. I understand that use of this equipment for private purposes is strictly prohibited.

I understand that this policy applies to me and I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment/contract with AbaQulusi Municipality.

I am aware that violations of this policy may subject me to disciplinary action, up to and including discharge from employment.

_____ _____

Employee/Contractor signature Date

_____

Employee/Contractor Printed Name

_____

Signature: Manager

FIREWALL MANAGEMENT POLICY

TABLE OF CONTENTS

16. OVERVIEW

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. Firewalls are used to separate networks with differing security requirements, such as the Internet and an internal network that houses servers with sensitive data. Organisations should use firewalls wherever their internal networks and systems interface with external networks and systems, and where security requirements vary among their internal networks.

A firewall policy defines how an organisation's firewall should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications and content types based on the organisation's information security policies.

17. PURPOSE

The purpose of this policy is to describe how the firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for users.

18. SCOPE

This policy is applicable to all business units that cause computing devices to be connected to the AbaQulusi Municipality's network.

19. POLICY

Installation of the Firewall and Requirements

4.1.1. The AbaQulusi Municipality's firewall runs on the CentOS operating system. In addition, Webmin is the interface used to manage the firewall.

4.1.2. When implementing the firewall:

4.1.2.1. Permitted connection and protocols, besides for those pre-approved connections, through the firewall must be explicitly defined and approved;

4.1.2.2. The firewall must be configured by default to prohibit all that is not explicitly permitted;

4.1.2.3. The firewall must be managed from a physically secure location;

4.1.2.4. Configuration and log files must be protected against unauthorised access. The integrity of these logs must be protected using checksums, digital signatures or similar measures;

4.1.2.5. The firewall must run on a dedicated machine, which performs no other function; and

4.1.2.6. The firewall must have only the bare minimum software and services resident to reduce the chances of security compromises.

4.1.3. THE FIREWALL WILL AT A MINIMUM PERFORM THE FOLLOWING SECURITY SERVICES:

4.1.3.1. Access control between the trusted internal network and untrusted external networks.

4.1.3.2. Block unwanted traffic as determined by the firewall rule set.

4.1.3.3. Hide vulnerable internal systems from the Internet.

4.1.3.4. Hide information, such as system names, network topologies, and internal user IDs, from the Internet.

4.1.3.5. Log traffic to and from the internal network.

4.1.3.6. Provide robust authentication.

4.1.3.7. Provide virtual private network (VPN) connectivity.

6.2.1.

4.1.4. THE APPROACH ADOPTED TO DEFINE FIREWALL RULE SETS IS THAT ALL SERVICES WILL BE DENIED BY THE FIREWALL UNLESS EXPRESSLY PERMITTED IN THIS POLICY.

6.2.2.

4.1.5. THE FIREWALL PERMITS THE FOLLOWING OUTBOUND AND INBOUND INTERNET TRAFFIC.

4.1.5.1. Outbound – All Internet traffic to hosts and services outside of the AbaQulusi Municipality.

4.1.5.2. Inbound – Only Internet traffic from outside the AbaQulusi Municipality that supports the mission of the AbaQulusi Municipality.

4.1.6. Only necessary protocols should be permitted and all unnecessary IP protocols should be denied by default.

4.1.7. Firewall accounts should be limited to only those that are absolutely necessary, such as the administrator.

4.1.8. Compilers, editors, and other program development tools should be removed from the firewall that could enable an unauthorised user to install malicious software or backdoors.

4.1.9. Any feature of the firewall that is not needed should be disabled, including other network access, user shells and applications.

4.1.10. Turn on full-logging at the firewall and review logs on a periodic basis. Logs should be reviewed by the ICT Manager.

4.1.11. Statistics on firewall usage should be readily available.

Firewall management and security requirements

4.2.1. All routed connections (including connections to third parties) and connections to the Internet, must be routed though a secure firewall server that has been approved by the municipality.

4.2.2. All firewall configurations must be approved.

4.2.3. Privileges to modify the functionality, connectivity and services supported by the firewall must be restricted to a few individuals with a business need for these privileges.

4.2.4. The ICT Manager maintains the implementation and maintenance of the firewall rules on the firewall through the assistance of the service provider, DC Data.

4.2.5. All changes to firewall configuration parameters, rule sets, enabled services and permitted connectivity must be formally logged and follow the change control process.

4.2.6. Current off line backup copies of the firewall configuration file, connectivity permission files, firewall systems administration procedural documentation and related files must be securely stored.

4.2.7. The approval and release of firewall updates (example configuration, version updates) is the responsibility of the ICT Manager, who decides on the appropriate level of testing and manner of release of such updates.

Firewall standards

5.1. OPERATING SYSTEM

5.1.1. The firewall must be installed on a hardened operating system (if server based).

5.2. REMOTE ACCESS

5.2.1. Under no circumstances must remote access to the firewall be supported over “un-trusted” networks without some form of strong authentication.

5.3. PROTOCOLS/SERVICES

5.3.1. Only the necessary services, protocols and applications must be run.
5.3.2. Default services must be checked for appropriateness on a regular basis.
5.3.3. The firewall server must only be used for firewall functions (if server based).
5.3.4. The following programs must never be run on a firewall (if server based):
5.3.4.1. Remote Administration Tools (PCAnywhere, Carbon Copy, etc) – unless precautions have been made to prevent unauthorised access and approved;

5.3.4.2. Telnet server;

5.3.4.3. FTP server; and

5.3.4.4. Mail server/ service.

5.3.5. Allowed protocols and services must be documented with valid business reasons.

Rule base

6.1. The rule base must deny everything, allowing only that which is specifically authorised.

6.2. A stealth rule must be in place that drops (not rejects) any packets directed towards the firewall. This will ensure that nobody can directly connect or communicate to the firewall, other than administrators that are authorised.

Firewall Settings

1.1.1 IP forwarded must be disabled.

1.1.2 Anti- spoofing must be enabled

1.1.3 ICMP must be disabled.

Connection

8.1. Obtain authorised approval for the connections and protocols that are being allowed through the firewall.

Location

9.1. The firewall is located within the server racks in the computer room of the municipality and managed by the ICT Manager with assistance from the service provider, DC Data.

Monitoring of Firewall

10.1.1. The firewall is monitored by the ICT Manager and through the assistance of theservice provider, DC Data.

ENFORCEMENT

11.1. Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanctions against the employee concerned and such sanctions may lead to termination of the employee's employment contract, depending on the circumstance and the gravity of the transgression.

11.2. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user, and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the employee.

GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY FRAMEWORK

TABLE OF CONTENTS

20. INTRODUCTION

The Public Service Corporate Governance of Information and Communication Technology Policy Framework (2012) stipulates that COBIT should be adapted and implemented as the Governance of ICT Framework on the Governance of ICT layer.

COBIT will enable the municipality to achieve their strategic goals by deriving optimal value from ICT through the realisation of benefits and optimising resources and risk.

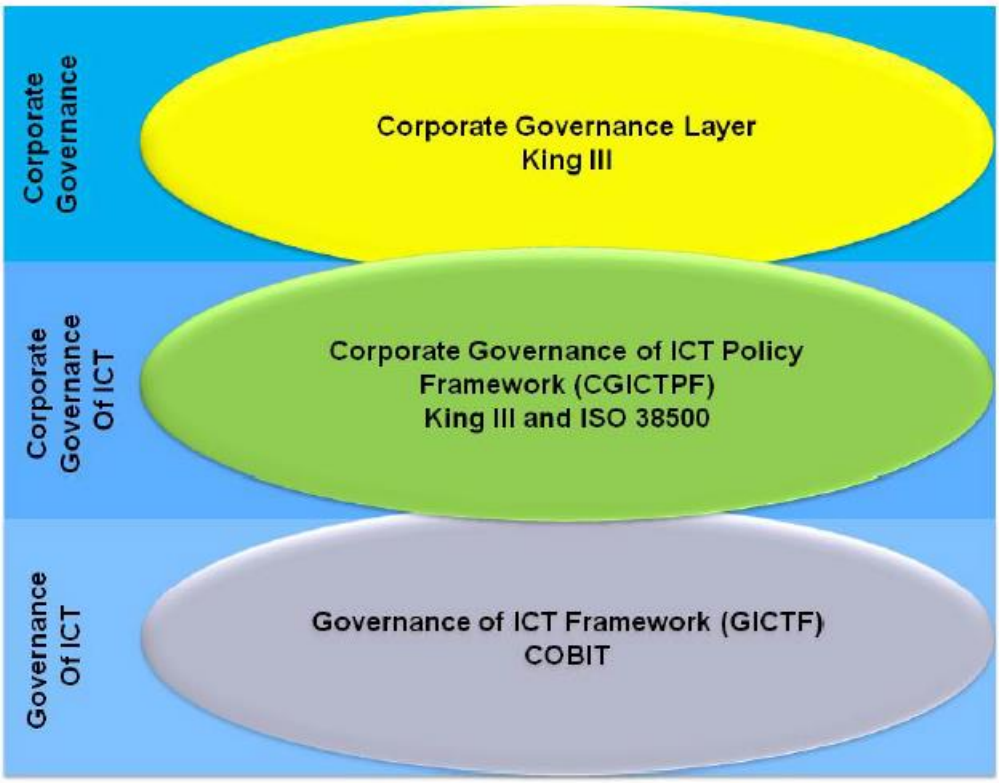
21. BACKGROUND ON COBIT

As a set of Governance of ICT and management processes, COBIT will provide managers, ICT users and auditors with the following:

a. Standard indicators;
b. Processes for implementing the Governance of ICT;
c. Good practice to maximise the corporate value in using ICT.
d. Identification of the accountability and responsibilities of business and ICT process owners;
e. Metrics to measure the achievement of the ICT-related goals; and
f. A model to measure governance of ICT process maturity.

22. GOVERNANCE OF ICT FRAMEWORK

The figure below demonstrates the different governance layers with their related frameworks and standards. The framework takes into consideration standards and practices such as the King III Code, ISO 38 500 standard and COBIT 5.



Source: DPSA – Public Service Corporate Governance of Information and Communication Technology Policy Framework (2012).

Implementation Guidelines, which are still to be published by the DPSA, will provide guidance on the implementation of COBIT as the process framework for the Governance of ICT in the municipality.

Public Service Corporate Governance of Information and Communication Technology Policy Framework prescribes that the Governance of ICT Framework be informed by the COBIT 5 processes in the table below. The GITOC (2012) has adopted 12 minimum processes that should inform implementation.

The minimum COBIT 5 processes that AbaQulusi Municipality will implement are listed below:

COBIT 5 Process	Process Description
EDM01: Governance framework setting and maintenance	a. Analyse and articulate the requirements for the governance of IT and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the municipality's mission, goals and objectives.
APO01: Manage the ICT management framework	a. Clarify and maintain the governance of the municipality's IT mission and vision. b. Implement and maintain mechanisms and authorities to manage information and the use of IT in the municipality in support of governance objectives in line with guiding principles and policies.
APO02: Manage strategy	a. Provide a holistic view of the current business and IT environment, the future direction and the initiatives required to migrate to the desired future environment. b. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives.
APO03: Manage enterprise architecture	a. Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. b. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools and provide a linkage for these components. c. Improve alignment, increase agility, improve quality of information and generate potential cost savings

COBIT 5 Process	Process Description
	through initiatives such as re-use of building block components.
APO05: Manage portfolio	a. Execute the strategic direction set for investments in line with the enterprise architecture vision and the desired characteristics of the investment and related services portfolios and consider the different categories of investments and the resources and funding constraints. b. Evaluate, prioritise and balance programmes and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. c. Move selected programmes into the active services portfolio for execution. d. Monitor the performance of the overall portfolio of services and programmes, proposing adjustments as necessary in response to programme and service performance or changing municipality priorities.
APO10: Manage Suppliers	a. Manage IT-related services provided by all types of suppliers to meet the municipality's requirements, including the selection of suppliers, management of relationships, management of contracts and reviewing and monitoring of supplier performance for effectiveness and compliance.
APO12: Manage Risk	a. Continually identify, assess and reduce IT-related risk within levels of tolerance set by executive management.
APO13: Manage security	a. Define, operate and monitor a system for information security management.
BAI01: Manage programmes and projects	a. Manage all programmes and projects from the investment portfolio in alignment with the municipality's strategy and in a co-ordinated way. b. Initiate, plan, control and execute

COBIT 5 Process	Process Description
	programmes and projects and close with a post-implementation review.
DSS01: Manage operations	a. Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities.
DSS04: Manage continuity	a. Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the municipality.
MEA01: Monitor, evaluate and assess performance and conformance	a. Collect, validate and evaluate business, IT and process goals and metrics. b. Monitor that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.

As per the DPSA requirements, the following have also been addressed when developing the IT Governance Framework:

Area	Reference
• Processes	IT Processes will be informed by the relevant CoBIT areas as described above.
• Principles & Policies	High level principles have been included in the Corporate Governance of IT Policy and policies developed contain policy statements at a lower level.
• Organisational Structure	The governance structures from an IT perspective including their interactions with the overall governance arrangements of the Municipality are contained in the IT Charter
• Skills and Competencies	IT skills and competencies will be reviewed through the normal performance management systems of the Municipality and further training needs may be highlighted when developing the IT Strategy
• Culture & Behaviour	The expected or required behaviour of staff from an IT perspective is contained in the IT End User Security Policy
• Information	The appropriate handling and dissemination of information is covered in the IT End User Security and IT Security Policies
• Service Delivery Structure of ICT including functions and responsibilities	The structures, functions and responsibilities from an IT governance perspective are covered in the IT Charter.
• Stakeholders & Role-players	Stakeholders, roleplayers and their responsibilities in terms of decision making have been included in the IT Charter.
• Supplier Management • ICT Project Management • ICT Continuity Management • ICT Risk Management	Policies have been developed for all of the areas mentioned

HELP DESK AND INCIDENT MANAGEMENT POLICY

TABLE OF CONTENTS

1. Introduction

This policy describes the procedure to control the ICT process of managing the IT helpdesk and incidents at the AbaQulusi Municipality. The process covers incident identification, analysis, resolution and review as conducted by the IT helpdesk.

2. Purpose

The purpose of this policy is to establish a uniform process for incident management, and define the steps involved in responding to employee calls via the IT Helpdesk at AbaQulusi Municipality.

3. Key Objectives

3.1. Logging of the Call

3.1.1. Calls must be logged to the IT Helpdesk by the user either telephonically by calling extension 2213 or via email on helpdesk@abaqulusi.gov.za.

3.1.2. All calls to the IT Helpdesk are recorded on the CCM Helpdesk system by the Systems Support Officer.

3.1.3. Details such as the Call Reference Number, User's Name, User's contact details, Date and Time Logged, Nature of Issue and Priority Status are recorded by the Systems Support Officer on the CCM Helpdesk system.

3.1.4. The user must be issued with a reference number.

3.1.5. Calls must be classified on the CCM Helpdesk system as per the categories (compliant type) below:

3.1.5.1. Network;
3.1.5.2. Software;
3.1.5.3. Email;
3.1.5.4. Hardware;
3.1.5.5. User Administration;
3.1.5.6. Other.

3.2. Priority of Call

3.2.1. Calls logged/ incidents are classed as Priority 1, Priority 2, Priority 3, Priority 4 and Priority 5 based on the nature of the call logged.

3.2.2. The following timeframes will be assigned to the priority of the call:

3.2.2.1. Priority 1 - task must be completed within 4 business hours
3.2.2.2. Priority 2 - task must be completed within 12 business hours
3.2.2.3. Priority 3 - task must be completed within 24 business hours
3.2.2.4. Priority 4 - task must be completed within 5 business days
3.2.2.5. Priority 5 - task must be completed within 2 business weeks

3.2.3. Calls logged must be attended to and resolved timeously.

3.3. Person assigned to incident

3.3.1. All calls are assigned to the Information Technology Officer for resolution, however in his absence the Senior Information Technology Officer is required to resolve any calls logged/ incidents.

3.3.2. Upon resolution of the call, the person assigned must inform the IT Helpdesk to close the call on the IT Helpdesk system.

3.3.3. The date and time that the call is resolved is recorded together with any additional comments if needed.

3.4. Monthly review

3.4.1. A monthly review of calls and incidents logged on the IT Helpdesk system must be performed by the ICT Manager, indicating compliance, long outstanding calls and trends.

4. Enforcement

4.1. Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanctions against the employee concerned and such sanctions may lead to termination of the employee's employment contract, depending on the circumstance and the gravity of the transgression.

4.2. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user, and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the employee.

ICT CHANGE MANAGEMENT POLICY

TABLE OF CONTENTS

1. INTRODUCTION

IT Change Management is the practice of ensuring the delivery of ICT and municipal services is not impacted by infrastructure or software changes and that all changes are recorded and carried out in a planned and authorised manner. This includes ensuring there is a business reason for each change, identifying the specific configuration items and ICT services affected by the change, identifying those staff responsible for implementing the change, planning the change, testing the change and having a back-out plan should the change result in an unexpected failure.

2. OBJECTIVES

The goal of the ICT Change Management Policy is to define the requirements necessary to meet the following business objectives:

- Reduce the risk of business disruption from information systems and infrastructure changes.
- Improve communication among stakeholders that may initiate and / or be impacted by changes.
- Comply with internal control and regulatory requirements.

3. BACKGROUND

The goal of ICT Change Management is to manage the process of change to these systems through standardised methods and procedures, thereby limiting incidents related to change and improving day-to-day operations.

Without formal change management policies and governance there is scope for operational inefficiency in the municipality's systems.

4. SCOPE

This policy applies to all AbaQulusi Municipality employees, contractors and any other individuals involved in making changes to AbaQulusi Municipality's production, technical and information assets for which IT has accountability.

5. DEFINITIONS

Change:A change is any activity that occurs to any information resource where the status is different from a previously defined condition. This is applicable to all ICT hardware, communications equipment and software, business systems software, 'live' applications software and all documentation and procedures that are relevant to the running, support and maintenance of live systems. A change can also be initiated to resolve a critical problem.

User (s): For the purposes of this document any reference to 'user' or 'users' is referring to the business users who initiate the change request.

Emergency Change: An emergency change is an unexpected or unplanned change that will either minimise service disruption or restore service.

Change Management: is the process of developing a planned and documented approach to change in an organisation.
In the ITIL framework, Change Management is responsible for controlling change to all configuration items within the live environment, test and training environments, and all environments under the control of 'ICT Operations'.

Business owner: Manager of an organisational unit within AbaQulusi Municipality who bears responsibility for the acquisition, development and maintenance of production applications that process municipality information.

Configuration Items: A component within a system configuration that needs to be controlled e.g. PC, server, switch, and printer.

ITIL: United Kingdom's Office of Government Commerce Information Technology Infrastructure Library.

6. POLICY

Every change to AbaQulusi Municipality's production information resources is subject to the ICT ChangeManagement Policy and must follow the approved AbaQulusi MunicipalityICT Change ManagementProcedure.

6.1. Change Requests

6.1.1. A formal change request process must be initiated to ensure business owners and the ICT department follow a defined change process for all types of changes including changes to ICT infrastructure, ICT systems and applications.

6.1.2. All change requests must be logged on the IT Helpdesk system.

6.1.3. All change requests must have a unique reference number associated with the request.

6.1.4. All change requests must be prioritised (High, Medium or Low) based on the business and technical requirements, resources required and the legal, regulatory and contractual reasons for the requested change.

6.1.5. All change requests must be categorised (example business process, infrastructure, operating systems, networks, application systems) based on the need and urgency of the change.

6.2.Change Planning, Evaluation and Scheduling

4.7.

6.2.1. All changes must be planned, evaluated and scheduled.

6.2.2. A risk and impact analysis of the change must be performed and included in the planning and evaluation of change requests to ensure that all components and risks affected by the change have been identified and assessed.

6.2.3. A back-out plan must be documented for all changes.

6.3.Test Environment

6.3.1. The AbaQulusi Municipality must establish a secure test environment that is representative of the production environment.

6.3.2. The test environment must also be representative of the future business and operational landscape, including business process procedures and roles, likely

workload stress, operating systems, necessary application software, database management systems and network and computing infrastructure found in the production environment.

6.3.3. ICT Management must ensure that the test environment cannot interact with production systems.

6.4.Change Testing

6.4.1. Testing of changes must be performed prior to the change being implemented in the production environment and proof of testing must be retained as evidence.

6.4.2. User Acceptance Testing (UAT) must be performed to ensure that the user's requirements have been met.

6.5.Change Implementation

6.5.1. UAT approval must be obtained prior to a change been migrated to the production environment.

6.5.2. ICT Management must formally approve each change request prior to the implementation of the change in the production environment.

6.5.3. All changes must be communicated prior to implementation in the production environment.

6.5.4. All unsuccessful changes must be backed-out in accordance with the defined back-out plan.

6.6.Change Reporting

6.6.1. ICT Management must develop change status reports with performance metrics to enable management to review and monitor the status of changes.

6.6.2. ICT Management must monitor open changes to ensure that all approved changes are closed in a timely fashion.

6.6.3. ICT Management must maintain a tracking and reporting system for all change requests.

6.7.Change Documentation

6.7.1. Technical and user documentation must be updated to reflect changes made to information systems and related technology.

6.7.2. A central repository must exist to contain all relevant information on configuration items. This repository includes hardware, application software, middleware, parameters, documentation, procedures and tools for operating, accessing and using the systems and services.

6.7.3. ICT Management must retain change documentation and user documentation.

6.8. Emergency Changes

6.8.1. A procedure must exist to govern emergency changes to information systems and related technology.

6.8.2. Criteria that define an emergency change must be clearly documented and communicated.

6.8.3. Emergency changes must be documented.

6.8.4. Emergency changes must be approved by the ICT Manager.

7. SEGREGATION OF DUTIES

7.1. Segregation of Duties (SoD) must be practiced to ensure that no single individual has the authority to execute multiple conflicting tasks with potential to impact other systems or information; and that no single individual can execute conflicting end-to-end transactions.

7.2. Segregation of duties at AbaQulusi Municipality with regards to program changes must follow the guidelines as stipulated below:

The role of …	Must be independent of …
Requester	Implementer
Builder	Operators of the production environment
Builder	Tester
Builder	Implementer
Builder	At least one approver
Requester	At least one approver
Implementer	At least one approver
Implementer	Reviewer
Auditor	All participants of a specific change
Approver	All other roles listed above

8. CONTROLS

8.1. This policy document addresses the following control objectives:

Control Objective Name	Control Objective Detail
Change Standards and Procedures	Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.
Impact Assessment, Prioritisation and Authorisation	Ensure that all requests for changes are assessed in a structured way for impacts on the operational system and its functionality. This assessment should include categorisation and prioritisation of changes. Prior to migration to production, changes are authorised by the appropriate stakeholder.
Emergency Changes	Establish a process for defining, raising, assessing and authorising emergency changes that do not follow the established change process. Documentation and testing should be performed, possibly after implementation of the emergency change.
Change Status Tracking and Reporting	Establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.
Change Closure and Documentation	Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly. Establish a review process to ensure complete implementation of changes.
Configuration Repository and Baseline	Establish a central repository to contain all relevant information on configuration items. This repository includes hardware, application software, middleware, parameters, documentation, procedures and tools for operating, accessing and using the systems and services. Relevant information to consider is naming, version numbers and licensing details. A baseline of configuration items should be kept for every system and service as a checkpoint to which to return after changes.

9. CROSS-REFERENCE TO OTHER POLICIES AND PROCEDURES

9.1. ICT Change Management Procedure.

10. REFERENCE MATERIAL

10.1. ITIL v4 Framework; and

10.2. ISO/IEC 20000.

11. ACCOUNTABILITIES

11.1. RESPONSIBILITY

All employees, contractors, business owners and ICT staff are required to adhere to this policy. Non-compliance to this policy may lead to appropriate disciplinary action.

11.2. TRAINING PLAN

All business owners and managers are responsible for promoting individual employee awareness of and compliance with the municipality's IT Change Management policies and procedures.

11.3. COMPLIANCE

All employees, contractors, business owners and ICT staff have to comply.

ICT CHANGE MANAGEMENT PROCEDURE

Table of Contents

2. Introduction

ICT Change Management is the practice of ensuring the delivery of ICT and municipal services is not impacted by infrastructure or software changes and that all changes are recorded and carried out in a planned and authorised manner. This includes ensuring there is a business reason for each change, identifying the specific configuration items and ICT services affected by the change, identifying those staff responsible for implementing the change, planning the change, testing the change and having a back-out plan should the change result in an unexpected failure.

3. Objective

The goal of this ICT Change Management Procedure is to ensure that request's for changes to AbaQulusi Municipality's ICT Infrastructure and municipal services are assessed through the correct channels and follows the appropriate processes as per the ICT Change Management Policy in order to prevent any unauthorised changes or changes which have not been adequately tested from being promoted into the production environment.

4. Scope

This procedure document applies to all AbaQulusi Municipality employees, vendors and contractors responsible for the design, development, maintenance and operations of AbaQulusi Municipality's ICT Infrastructure and Business Systems.

5. Change Management Procedure

4.1. Normal Changes

Changes Performed by Service Providers and Internal Changes

4.1.1. To initiate the Change Request Process, a Change Request Form (Appendix A) must be completed by the Change Requester on the "USER" section of the form.

4.1.2. Once the Requestor has completed the "USER" section of the form and signs it off, the form must be approved and signed-off by the following individuals:

4.1.2.1. ICT Manager
4.1.2.2. Director Corporate Services

4.1.3. The ICT Manager must allocate a priority level to the change request to indicate its urgency as a business requirement.

4.1.4. There are two priority levels that may be selected for changes:

4.1.4.1. Normal Change – Normal priority for changes that will follow the standard change management process.
4.1.4.2. Emergency Change – High priority changes that need to be urgently implemented. Emergency changes must only be implemented to resolve an urgent business issue, such as production system(s) being down or when an important business function/process is affected and no other workaround is available. Emergency changes must follow the steps of the emergency change procedure in section 4.2 below.

4.1.5. The Change Request Form must be submitted to the IT Helpdesk.

4.1.6. The IT Helpdesk must verify the change request for completeness, relevance and authorisation, and log the change onto the Helpdesk system for tracking purposes.

4.1.7. The reference number provided by the Helpdesk system must be captured as the change reference number.

4.1.8. The form must be routed to the ICT Manager for approval.

4.1.9. The ICT Manager must review the change request, taking into consideration the potential risk and impact of the change.

4.1.10. Only once satisfied that the change should go ahead, the ICT Manager must sign-off the Change Request Form.

Changes Performed by Service Providers

4.1.11. The ICT Manager will grant the relevant service provider access to the system that the change will be performed on and the access will be restricted to the period that the change is scheduled for.

4.1.12. The approved Change Request Form must be submitted for action to the service provider responsible for system changes – this will subsequently kick-off the service providers change management process, and they will evaluate the change request and develop the change.

4.1.13. When testing, including user acceptance testing, of the change is successful and the change is ready for implementation, the ICT Manager must provide approval to implement the change in the production environment.

4.1.14. If the change is unsuccessful, the change must be backed-out as documented in the back-out plan, the help desk must be notified and the change must be closed on the Helpdesk system.

4.1.15. If the change is successful, the IT Helpdesk must be notified and the change must be closed on the Helpdesk system.

4.1.16. After the change has been closed, the ICT Manager will then revoke/disable the relevant service providers' access.

Internal Changes

4.1.17. Changes that will be done internally will need to be implemented in the test environment before been moved into the production environment.

4.1.18. After the change is successfully implemented in the test environment, the change will need to be tested and signed-off by the developer.

4.1.19. User Acceptance Testing must then be performed and sign-off obtained.

4.1.20. Approval must then be obtained from the ICT Manager to move the change into the production environment.

4.1.21. After approval has been obtained, the change will then be implemented in the production environment.

4.1.22. If the change is unsuccessful, the change must be backed-out as documented in the back-out plan, the help desk must be notified and the change must be closed on the Helpdesk system.

4.1.23. If the change is successful, the IT Helpdesk must be notified and the change must be closed on the Helpdesk system.

4.2.Emergency Changes

4.2.1. An emergency change is the highest priority change within the change management process and is required to be evaluated, assessed and approved/rejected in a short space of time.

4.2.2. Emergency changes must follow a streamlined process that still provides for retrospective review, approval and logging of changes.

4.2.3.The following key rules apply to emergency changes:

4.2.3.1. An emergency change must be logged as a as a high priority change.

4.2.3.2. All change request documentation may be completed retrospectively.

4.2.3.3. Approvals must however still be required as documented in the Emergency Change Request Procedures below.

4.2.3.4. The IT approval process must be completed within three (3) business days after the emergency change has been implemented.

4.2.4. To initiate the Emergency Change Request Process, the Change Request Form (Appendix A) must be completed by the Requestor. The “Emergency Change” box must be appropriately ticked on the form to indicate that it is an emergency change.

4.2.5. Once the Requestor has completed the “USER” section of the form, the request must be sent to the IT Helpdesk.

4.2.6. The IT Helpdesk must log the change onto the Helpdesk system for tracking purposes and inform the ICT Manager and the Director Corporate Services that a change has been prioritised as an Emergency Change.

4.2.7. The ICT Manager and Director Corporate Services must provide approval via email before the change can be implemented in the production environment.

4.2.8. Details of the emergency change request will be forwarded via email to the service provider responsible for system changes, authorising them to action and implement the change.

4.2.9. Developers from the service provider must action the change and perform the necessary testing procedures.

4.2.10. Once the emergency change has been implemented successfully, the service provider must notify the ICT Manager, Director Corporate Services and the IT Helpdesk via email.

4.2.11. The IT Helpdesk must notify the Change Requestor that the change has been implemented.

4.2.12. The ICT Manager must ensure that Change Management documentation (i.e. Change Request Form) is completed retrospectively within three (3) business days after the emergency change has been implemented.

4.2.13. The Change Request Form must be completed retrospectively and contain approvals as per the requirements of a normal change request.

4.2.14. The approval emails during the emergency change process must be attached to the Change Request documentation as supporting documentation.

4.2.15. The IT Helpdesk must update and close the Emergency Change Request call logged on the Helpdesk system.

6. Enforcement

Non-compliance, violation and disregard of this policy by any AbaQulusi Municipality employees, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual's employment contract, depending on the circumstance and the gravity of the transgression. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the individual and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the individual.

7. Appendices

Change Management Request Form

Appendix A – Change Request Form

A. USER

Requested by: _____ **Signature:** _____

Date:_____/_____/_____

Type of Request:

Software new ☐ Software Change ☐ Report new ☐ Report Change ☐

Data Change ☐ Data New ☐ General query ☐ Training ☐

Hardware ☐ Other ☐ If other, specify _____

System:

_____

Description of Request:

_____

_____

_____

Authorised by ICT Manager: _____ **Signature:** _____

Date:_____/_____/_____

Prioritisation Level:

Normal ☐ Emergency ☐

Authorised by HOD: _____ **Signature:** _____

Date:_____/_____/_____

B. HELPDESK LOGGING
Change Ref. #:_____ **Captured on Helpdesk System by:** _____ **Signature:**_____ **Proceed with Change** Yes☐ No ☐ **Reviewed by ICT Manager:** _____ **Signature:**_____ **Date:**_____/_____/_____
D. TESTING
Testing successful? Yes☐ No ☐ **Results of Testing Reviewed by (ICT Manager):** **Signature:** _____ **Date:**_____/_____/_____
E. USER ACCEPTANCE TESTING
Signed off by (Requestor): _____ **Signature:**_____ **Date:**_____/_____/_____
F. IMPLEMENTATION
ICT Manager Approval: _____ **Signature:**_____ **Date:**_____/_____/_____ **Implementer:** _____ **Signature:**_____ **Date:**_____/_____/_____ **Change implemented successfully?** Yes☐ No ☐

INFORMATION COMMUNICATION AND TECHNOLOGY CHARTER

TABLE OF CONTENTS

1. PURPOSE

AbaQulusi Municipality has a dependency on ICT to enable its business processes. Due to the critical nature of ICT and the intellectual and other information resources that are exposed through technology channels, ICT governance now represents an essential component in ensuring the efficient and secure operation of the business.

Chapter 5 of King III provides that directors, in exercising their duty of care, should ensure that prudent and reasonable steps have been taken with respect to ICT Governance. Chapter 5 sets out the following 7 principles:

a. Council should be responsible for Information Technology (IT) Governance;
b. ICT should be aligned with the performance and sustainability objectives of the municipality;
c. Council should delegate to management the responsibility for the implementation of an ICT governance framework;
d. Council should monitor and evaluate significant ICT investments and expenditure;
e. ICT should form an integral part of the municipality's risk management;
f. Council should ensure that information assets are managed effectively; and
g. A risk committee and audit committee should assist Council in carrying out its ICT responsibilities.

Within Principle 5.7.2, King III recommends that AbaQulusi Municipality's Council ("Council") establish an ICT Charter. The ICT Charter outlines the *decision-making rights and accountability framework for IT governance* that will enable the *desirable culture in the use of ICT* within the municipality. This document will serve as the ICT Charter for AbaQulusi Municipality.

In addition, King III allows Council to delegate to management or to other Council committees the responsibility for the implementation and monitoring of ICT governance. The ICT Charter document also clarifies delegated responsibilities.

2. DESIRABLE CULTURE IN THE USE OF ICT

Council defines the desirable culture in the use of ICT hereunder. The decision making rights and accountability framework defined in the remainder of the document is designed to achieve these 10 objectives.

1. The activities and functions of the ICT Strategy are aligned to the business strategy. Opportunities to improve the use of ICT within AbaQulusi Municipality are identified and exploited.
2. The optimal investment is made in ICT, costs are managed and the return on investment is measured.
3. Synergies between ICT initiatives are enabled and ICT choices are in the best interest of the municipality as a whole and not only those of individual business units.
4. ICT services are sourced optimally and legitimately.
5. ICT risks are identified and adequately addressed. Assurance is obtained to ensure that an ICT control framework is in place to address ICT risks.
6. Information, ICT assets and intellectual property contained in ICT systems are protected and effectively managed and used.
7. ICT has adequate business resilience arrangements in place for disaster recovery.
8. Information Management is a joint ICT and business responsibility.
9. ICT use conforms to ICT related laws and related rules, codes and standards are considered.
10. ICT use is sustainable with respect to the environment.

3. DECISION MAKING RIGHTS AND ACCOUNTABILITY

The Municipal Manager has responsibility to establish an ICT department for AbaQulusi Municipality.

Council identifies with the following decision making domains:

a. ICT Strategy;
b. General ICT Management and Administration;
c. ICT Governance, Risk and Compliance;
d. ICT Investments and Projects;
e. ICT Sourcing;
f. ICT Operations;
g. Business and ICT Architecture;
h. Information;
i. Application Management; and
j. ICT Security.

Council grants decision making rights within the ICT Department by using the following RACI Chart:

IT Decision Category	Decision Making Committee	Responsibility					
		Municipal Manager	Director Corporate Services	ICT Manager	Department Heads	EXCO	Audit and Risk Committee
ICT Governance, Risk and Compliance	ICT Steering Committee	A	R	R	I	I	I/C
ICT Strategy	ICT Steering Committee	A	R	R	I/C	C	I
Application Management	ICT Steering Committee	A	A	R	I/C	I	I
Information	ICT Steering Committee	A	C	R	I/C	I	I
Business and ICT Architecture	ICT Steering Committee	A	C	R	C	C	I
ICT Investments and Projects	ICT Steering Committee	A	R	R/C	I/C	C	I
ICT Sourcing	ICT Steering Committee	A	C	R	I	I	I
ICT Security	ICT Steering Committee	A	C	R	I	I	C
ICT Operations	ICT Steering Committee	A	C	R	I	I	I
General ICT Management and Administration	ICT Steering Committee	A	C	R	I	I	I

A RACI Model is a tool used for identifying roles and responsibilities.

Key:

R	Responsible
A	Accountable
C	Consulted
I	Informed

3.1. ICT Steering Committee

An ICT Steering Committee will be established to take decisions in the following areas:

ICT Governance, Risk and Compliance

- Ensure the implementation of the ICT Charter, including the defined ICT governance structures and CGICT policy.
- Maintain the ICT Charter and CGICT policy.
- Receive and act upon direction from the Audit and Risk Committee relating to ICT governance.
- Ensure that an ICT internal control framework is implemented.
- Ensure that ICT principles, policies, procedures and standards are defined and implemented.
- Approval of ICT principles, policies, procedures and standards.
- Ensure the promotion of an ethical ICT governance culture and awareness of a common IT language.
- Ensure that the municipality has adequate business resilience arrangements in place for ICT disaster recovery.
- Ensure that appropriate processes are followed for the identification, assessment and management of ICT Risks.
- Ensure compliance with relevant ICT laws and related rules, codes and standards.
- Ensure that a process is established for legal review of ICT contracts.
- Ensure that IT financial governance (e.g. sign-off levels, budget principles such as depreciation rules) is adhered to within ICT.
- Ensure the municipal sustainability strategy is supported by ICT strategies.
- Obtain assurance on the ICT governance and controls supporting significant outsourced ICT services.
- Receive and act upon independent ICT audit reports.
- Provide a report on ICT to Council to provide assurance that their responsibilities relating to King III have been implemented in terms of the following:
    - Value derived from ICT, measured against ICT performance criteria;
    - ICT risks;
    - ICT security and continuity, including data privacy;
    - ICT projects;
    - ICT cost and major investments;
    - ICT strategy and progress on IT strategy plan; and
    - ICT governance and control.
- Overseeing the ICT implementation of the ICT Governance framework, knowledge and information management and strategic sourcing.

- Ensure that a process is in place to identify and position strategic ICT initiatives and services which will best contribute to the achievement of municipal objectives and are agile and adaptive enough to support changes in the municipal strategy.
- Resolve conflicting business priorities.
- Ensure that an ICT strategy is prepared.
- Ensure that business units understand the importance of common ICT standards and implications of non-compliance.
- Ensure implementation of the ICT strategy and monitoring of outcomes.
- Monitoring ICT performance and dealing with performance issues.

General ICT Management and Administration

- Review and approve major decisions relating to General ICT Management and Administration, these include ICT human resources, ICT financial management and marketing of ICT services to the other business units (business relationship management).

Business and ICT Architecture

- Ensure research and innovation in terms of ICT trends and emerging technologies are performed.
- Ensuring business and ICT alignment with respect to the structuring, acquisition, control, protection, delivery and value enhancement of data and information assets to the municipality.

Information

- Information lifecycle policies and procedures, from creation to destruction, of both electronic and hard-copy documents.
- Allocation of ownership and custodianship rights to data and information to facilitate accountability and responsibility for decision making.
- Access to information (including information security levels).
- Information classification.

Application Management

- Review and approve major decisions affecting application management.
- Application management encompasses the management of the configuration; implementation, hosting, support and maintenance of applications (e.g. license management).

ICT Operations

- Review and approve major decisions affecting ICT operations.
- ICT operations encompass the delivery of required services, which includes service delivery, management of security and continuity, service support for users and management of data and operational facilities.
- Provide input and approve the development of an ICT Plan, ICT Implementation Plan, ICT Operational Plan, Governance and Management of ICT Framework and ICT Project Program.
- Coordinate implementation of the ICT Plan, ICT Implementation Plan, ICT Operational Plan and ICT Project Program.

ICT Sourcing

- Ensure the implementation of good governance principles to be applied for the acquisition of ICT goods and services.
- Ensure compliance with the defined Request for Proposal (RFP) process.
- Ratification of the RFP outcome.

ICT Investments and Projects

- Monitor and evaluate significant ICT investments and expenditure.
- Prioritise and approve ICT investment requests (ICT projects) within the delegated approval framework, ensuring the right balance between initiatives that run the current municipal business, grow the existing municipal business and have the potential to transform the municipality.
- Ensure that the size of the ICT budget is appropriate.
- Ensure that appropriate project management principles and frameworks are applied to all significant projects.
- Ensure that effective review processes are performed by independent experts on all municipal critical projects.

ICT Security

- Ensure compliance with ICT Security related laws and related rules, codes and standards.
- Ensure that the intellectual property contained in information systems is protected.
- Review and approve ICT security risk acceptance decisions.
- Review and approve ICT security policies, principles and standards.

3.2. Membership

- Municipal Manager;
- Director Corporate Services;
- Chief Financial Officer;
- ICT Manager (Chair);
- Information Technology Officer;
- Other department (portfolio) heads (invitation basis)
- Any outside expert (invitation basis)

3.3. Meetings

- The committee will meet at least four times a year, with more frequent meetings, as circumstances require.
- The quorum for decisions is at least 50% of the invited members.
- The committee shall keep an attendance register and minutes of meetings.
- Submit the minutes of meetings to the Corporate Services Portfolio Committee within two weeks.

4. COUNCIL AND EXCO RESPONSIBILITIES

Council/EXCO retains the following responsibilities for ICT governance.

4.1. ABAQULUSI MUNICIPALITY EXECUTIVE COMMITTEE

The Committee will carry out the following responsibilities:

- Direct and control ICT through the establishment of an ICT governance framework, embedded in this ICT Charter.
- Receive and act upon the Council report on ICT developed by the ICT Steering Committee to assure Council that their responsibilities relating to King III have sufficiently been implemented.
- Submit the Council report on ICT, or summaries thereof, to Council.
- Obtain appropriate assurance that controls are in place and effective in addressing ICT risk.
- Ensure that ICT risks are identified, assessed and mitigated through an ICT control framework.
- Consider ICT as it relates to financial reporting and the going concern of the municipality.
- Consider the use of technology to improve audit coverage and efficiency.

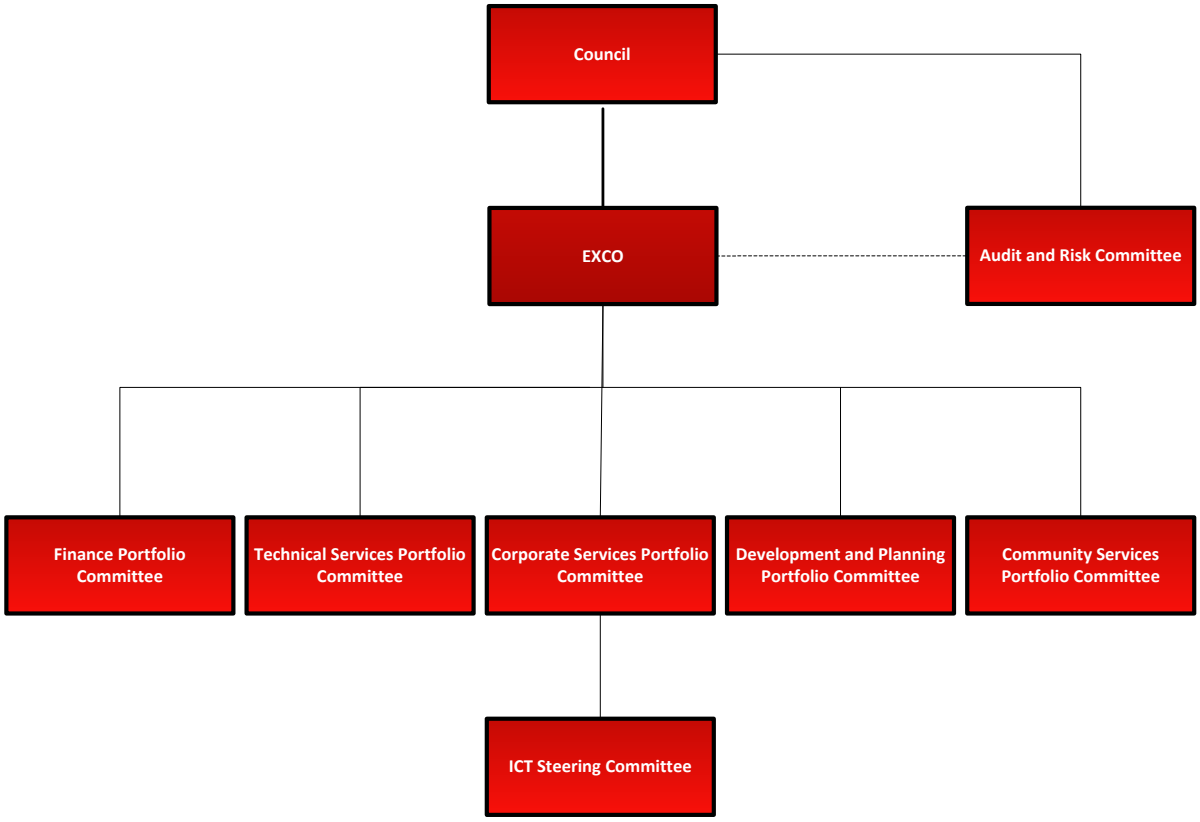
4.2. ABAQULUSI MUNICIPALITY COUNCIL

Council will retain accountability for ICT governance. Council will carry out the following responsibilities:

- Understand the strategic importance of ICT, assume responsibility for the governance of ICT and place it on the Council agenda.
- Receive and act upon Council level ICT reporting received from the Executive Committee.
- Satisfy that its responsibilities relating to King III have sufficiently been implemented.

5. RELATIONSHIP BETWEEN GOVERNANCE STRUCTURES

The relationship between Council and other Committee structures are illustrated below:



6. IT STANDARDS

6.1. COBIT

Principle 5.1.3 of the King III Report on Governance recommends that an IT internal control framework be adopted and implemented. CoBIT is also the recommended by the Department of Public Service & Administration as per the Implementation Guideline for Information & Communication Technology Policy Framework.

CobiT is an internationally recognised IT control framework which is published by the Information Systems Audit and Control Association (ISACA). ISACA asserts that it is a non-profit professional association with more than 47,000 members in more than 140 countries.

Council endorses that CobiT will be adopted and used as a reference when considering the development of the ICT internal control framework.

6.2. ISO 27000

Principle 5.6.3 of the King III Report on Governance recommends that an Information Security Management System (ISMS) be developed and implemented. The ISO 27000 series is currently the most recognised Information Security standard. The series include an ISMS specification (ISO 27001) as well as relevant security best practices (ISO 27002).

Council endorses that ISO 27000 will be adopted and used as a reference when considering the development of the ISMS to achieve King III Report on Governance compliance.

7. RISK ASSESSMENT & MITIGATION

A risk management policy for IT will be drafted to cater for IT Risks, this policy will be in-line with the Enterprise Risk Management Policy that has been adopted by the AbaQulusi Municipality.

Based on the existing governance structures, the ICT Steering Committee will deal with ICT Risks raised by the Director Corporate Services and the ICT Manager. These will be communicated to the Audit and Risk Committee via the Corporate Services Portfolio Committee and EXCO. In addition, the Corporate Services Portfolio Committee will raise and communicate ICT Risks to EXCO and Council.

8. APPROVAL

This Charter was approved by the following:

_____ _____

Council **Date**

_____ _____

Chairman of the Executive Committee **Date**

_____ _____

Chairman of the Corporate Services Portfolio Committee **Date**

_____ _____

AbaQulusi Municipal Manager **Date**

ICT PROJECT MANAGEMENT POLICY

TABLE OF CONTENTS

23. SCOPE

This policy applies to all employees of AbaQulusi Municipality and all parties that interact with the information and systems of the municipality.

24. POLICY

ICT programmes and projects must be managed in a co-ordinated and structured manner to enable improvement on the quality and value of project deliverables and reduce the risk of unexpected delays and increased costs.

25. ROLES AND RESPONSIBILITIES

ICT Steering Committee	Must be consulted on decisions relating to identification and selection of ICT projects and must be informed of results of monitoring activities.
ICT Manager	Must be consulted throughout all the phases of the Project Management lifecycle. Takes responsibility for initiating the project, monitoring of project execution, ensuring project quality and management of project risk. Ultimately accountable for ensuring that all projects are managed efficiently and effectively throughout the municipality. Responsible for documenting project planning/execution documents and ensuring that the all project phases conform to the project management methodology of the municipality.

26. PROJECT INITIATION

4.1. AbaQulusi Municipality defines an IT project as follows:

4.1.1. Has a monetary value greater than R100000 OR

4.1.2. Where multiple end users are affected.

4.2. The initiative of the programme or project must be identified by the ICT Manager.

4.3. Once the initiative is identified, a feasibility analysis must be conducted by the ICT Manager and a request with full specifications must be made to the ICT Steering Committee for approval.

4.4. Based on the results of the ICT Steering Committee, the normal procurement process would apply for the sourcing of the services of a suitable vendor.

27. PROJECT EXECUTION

5.1. Once a vendor is appointed, a Project Team should be established which includes members of the ICT Steering Committee together with key representatives from the municipality who are affected by the project.

5.2. Regular meetings must be scheduled for the duration of the project.

5.3. The frequency of meetings will be determined by the Project Team.

5.4. A detailed project plan with key milestones and dependencies must be developed.

5.5. The project plan must be discussed at project meetings and will be used to track the project.

28. QUALITY ASSURANCE AND TESTING

6.1. The municipality is responsible for performing internal testing procedures as stipulated in the ICT Change Management Policy to ensure that the project deliverables have met the specified requirements.

6.2. Once project activities are completed, ICT must perform testing and Quality Assurance procedures on the deliverable(s).

6.3. User Acceptance Testing must also be completed by users, and this must be evidenced by sign-off.

6.4. Any errors identified during testing must be communicated to the vendor for resolution, and internal testing procedures must be repeated thereafter.

29. PROJECT IMPLEMENTATION AND CLOSURE

7.1. The ICT Manager and/or Director Corporate Services must provide approval before project implementation activities take place.

30. MONITORING

8.1. The ICT Manager must monitor project processes associated with initiating, planning, executing, and closing. Corrective and preventive actions must be taken to control the project performance.

8.2. The ICT Manager must document and maintain an issues log for the duration of the project.

8.3. A formal close out report must be developed by the project team at the end of the project.

8.4. The report must map back to the initial benefits documented in the feasibility analysis to ensure that the project has achieved them.

8.5. Areas of improvement based on how the project ran must be documented for future reference.

31. ENFORCEMENT

9.1. Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanctions against the employee concerned and such sanctions may lead to

termination of the employee's employment contract, depending on the circumstance and the gravity of the transgression.

9.2. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user, and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the employee.

ICT RISK MANAGEMENT POLICY

TABLE OF CONTENTS

1. INTRODUCTION

This policy applies to all employees of AbaQulusi Municipality and all parties that interact with the information and systems of the municipality.

2. Policy Statement

As a government institution, AbaQulusi Municipality must implement and support risk management relating to information systems. This includes reducing ICT-related risk as well as integrating the management of ICT-related risk with the municipality's overall risk management strategy.

3. Roles and Responsibilities

ICT Manager:	The ICT Manager must ensure that effective ICT Risk Management is established within the ICT Department.
Municipal Manager:	Risk management is a key responsibility of management. To achieve its business objectives, management should ensure that sound risk management processes are in place and functioning. The Municipal Manager hasan overall responsibility for managing risks related to the municipality's objectives and risk management. The Municipal Manager must ensure the establishment and maintenance of effective, efficient and transparent systems of financial and risk management.

4. Risk Management Evaluation

4.1. The level of ICT-related risk that the municipality is willing to accept in pursuit of its objectives (risk appetite) must be determined.

4.1.5.

4.2. ICT risk tolerance thresholds must be evaluated and approved based on the municipality's acceptable risk and opportunity levels.

4.1.6.

4.3. The ICT environment must be subject to risk assessments and evaluation to ensure compliance with national standards and legislation.

4.1.7.

4.4. Periodic ICT risk assessments must take place to identify new or emerging risk issues and to gain an understanding of the internal and external risk factors.

4.1.8.

4.5. Risk data relating to ICT risks of the municipality's internal and external operating environment must be recorded. These internal and external factors may include:

External Factors	**Natural environment**	Risks might include such natural disasters as flood, fire or earthquake and sustainable development.
	Political	Risks might include newly elected government officials, political agendas and new legislation and regulations. The influence of international governments and other governing bodies.

4.1.9.

Internal Factors	**Infrastructure**	Risks might include unexpected repair costs, or equipment incapable of supporting production demand.
	Human resource	Risks might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behaviour.
	Process	Risks might include product quality deficiencies, unexpected downtime, or service delays.
	Technology	Risks might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications.
	Governance and accountability frameworks	Values and ethics, transparency, policies, procedures and processes.

5. Establishment of Risk Management

5.1. The municipality must implement appropriate measures to identify and respond to changing and new risks.

5.2. The municipality must take appropriate steps to proactively identify ICT risk, opportunity and potential business impacts.

5.3. Risk communication plans and risk action plans must be developed to cover all relevant business units.

5.4. Changing and new risks must be promptly responded to, reported to the appropriate levels of management and, where necessary, discussed during the ICT Steering Committee or Audit and Risk Committee meetings.

5.5. The approach, capturing and reporting of measurement activities against goals/metrics must be approved.

5.6. The key goals and metrics must be identified for the governance and management processes that are included in the risk assessment.

5.7. ICT Risk Assessments must take place at least on an annual basis.

5.8. ICT Risk Assessments must be conducted on the municipality's environment according to the ICT Risk Management Policy and the Enterprise Risk Management (ERM) Policy adopted by the municipality.

6. IT RISK REGISTER AND REPORTING

6.1. A risk register of ICT risks must be maintained and updated with results from risk assessments.

6.2. The following minimum information is to be maintained and recorded on the risk register for ICT risks. Other columns on the electronic risk register will automatically populate themselves if the information below is captured.

6.2.1. Priority;
6.2.2. Risk Name;
6.2.3. Causes;
6.2.4. Risk owner;
6.2.5. Existing Controls;
6.2.6. Control Strength;
6.2.7. Desired Control Strengths
6.2.8. Risk Improvement Plan;
6.2.9. Risk Improvement Plan Owner;
6.2.10. Target Date; and
6.2.11. Risk Improvement Plan Progress.

6.3. The detail contained on the risk register must be used as the reporting tool to view and track the state of ICT risk management at the municipality.

6.4. The electronic ICT Risk Register will be maintained by the ICT Manager.

6.5. The following table contains the Risk Register work sheet meanings:

IT Risk Register Work Sheets	**Meanings**
Risk Register - Main	All Risks need to be captured into this worksheet
Risk Register – Top 15	Contains the top 15 ICT Risks (automatically populated)
Risk Metrics	Measures and explanations of ICT Risks
Graphs – Inherent	The risk that an activity would pose if no controls or other mitigating factors were in place (risk before controls) (automatically populated)
Graphs – Residual	The risk that remains after controls are taken into account (the risk after controls). (automatically populated)

7. Monitoring of Risk Management

7.1. The risk register must be monitored to determine the extent of it being managed within the municipality's risk appetite threshold.

7.2. Key goals and metrics of risk governance and management processes must be monitored against targets to identify deviations and requirements for remedial actions.

7.3. Key management must be able to review the municipality's progress towards achieving ICT risk management goals.

7.4. Risk management issues must be reported to EXCO and/or the Municipal Manager where necessary.

8. Responding to Risk Events

8.1. Risk events are events that can potentially have a negative impact on the municipality's ICT environment, which could lead to inefficiencies or potential monetary/data losses. Risk events can be categorised as recurring events or non-recurring events.

8.2. A cost-benefit analysis of potential risk response options must be performed for the optimal response actions to be selected.

8.3. In determining the appropriate responses, management must consider:

8.3.1. Evaluating the effectiveness of current measures in place to reduce the risk to an acceptable level;

8.3.2. Considering the control measures of leading practices and those implemented by other government institutions, provincial departments or local authorities that could be used to mitigate the risk more effectively.

8.4. A high-level plan must be documented to implement key controls to mitigate identified risks.

8.5. Controls that must be selected must include both Technical controls (access control systems, firewalls, etc) and Non-Technical controls (policies and procedures etc).

ICT SECURITY POLICY

TABLE OF CONTENTS

INTRODUCTION

Computers enable employees of AbaQulusi Municipality to conduct the organisation's day-to-day business activities more effectively and efficiently. In addition, computers also allow employees greater access to organisational resources and information. In order to promote a working environment that is conducive to teamwork and productivity, it is essential that all users understand their roles and responsibilities with regards to Information Communication Technology (ICT) security and adhere to the security requirements of AbaQulusi Municipality. IT security is therefore characterised as the preservation of:

- **Confidentiality** – Ensuring that information is only accessible to those individuals who are duly authorised to have access to it.
- **Integrity** – Safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – Ensuring that authorised users have access to information and associated assets as and when required.

As such, municipalities have different uses for their respective IT systems. The installation of AbaQulusi Municipality's IT network represents a significant IT investment and so IT equipment must be utilised in the best interest of, and be of benefit to, AbaQulusi Municipality.

1. OBJECTIVES

The objectives of the ICT Security Policy are to:

2.1. Clarify to all users their responsibilities regarding the security of AbaQulusi Municipality's information and computing resources.
2.2. Define the potential risks and dangers for AbaQulusi Municipality in the event of misappropriation and abuse of computing equipment by users.
2.3. Maintain an appropriate level of physical and logical security to safeguard IT systems and resources against unauthorised use, modification, disclosure or loss to preserve the integrity of the AbaQulusi Municipality IT environment.
2.4. Regulate the professional and effective use of computing equipment within AbaQulusi Municipality, as well as between AbaQulusi Municipality and its external entities.
2.5. Establish a standard for creation of User ID's and strong passwords, the protection of those passwords, and the frequency of change thereof.
2.6. Identify the persons responsible for maintaining the security requirements.
2.7. Establish management direction, basis of procedures and requirements to ensure the appropriate protection of AbaQulusi Municipality's information and equipment resources by any means.
2.8. Ensure that this investment in information and equipment resources is properly managed.
2.9. Ensure that the system is optimally utilized in its full capacity to the best advantage of AbaQulusi Municipality.

2. APPOINTMENT OF ICT STEERING COMMITTEE

AbaQulusi Municipality shall appoint an ICT Steering Committee that must meet at least quarterly to discuss IT-related improvements or changes in the ICT environment and infrastructure.

3. SCOPE

This policy applies to all employees, consultants and temporary staff who access AbaQulusi Municipality's computer networks with an organisation-owned or personal workstation and are responsible for an account (or any form of access that supports or requires a User ID and a password) on any system that resides at any AbaQulusi Municipality facility, has access to the network, or stores any non-public organisational information.All employees need to be aware of security risks and vulnerabilities in order to create organisation-wide security consciousness. Therefore, security awareness and training programmes shall be initiated and each employee shall be required to receive the necessary Information Security awareness and training provided by AbaQulusi Municipality.

4. ADMINISTRATIVE CONTROLS

5.1. General Controls

5.1.1. The ICT Manager will, on recommendation of the ICT Steering Committee, issue guidelines on the use and application of AbaQulusi Municipality's network and shall monitor compliance with these guidelines, which must be strictly adhered to by all users of any IT systems.

5.1.2. The required administrative controls applicable to the system will be included in these guidelines and will comprise the following:

5.1.2.1. Physical controls over computer hardware, backups and software;
5.1.2.2. Access controls;
5.1.2.3. Data security controls; and
5.1.2.4. Internet and email usage controls.

5.2. Programming and Documentation Standards

5.2.1. Only the ICT Manager, on recommendation of the ICT Steering Committee, may liaise with IT software suppliers to provide programmers for AbaQulusi Municipality's use and to have such programmers developed further or amended.

5.2.2. The ICT Manager shall keep a register of all such requests for amendment and/or enhancement of AbaQulusi Municipality software and hardware, and shall inform the relevant users of any changes.

5.3. Insurance

5.3.1. The Finance department shall ensure that appropriate and adequate insurance cover is obtained in respect of all components of AbaQulusiMunicipality's ICT operations.

5.4. Reporting

5.4.1. The ICT Manager shall report to the Director of Corporate Services on the general use and application of the IT network, indicating in such report whether existing administrative controls need to be reviewed or amended, specifying operational problems of material importance which have arisen during the month and quarter to which the report relates, and indicating how such problems have been or are being addressed.

5.5. Audits

5.5.1. The ICT Manager, in consultation with the Director of Corporate Services, shall arrange audits of the IT systems on a periodic basis.

5.5.2. These audits may be conducted by either the internal or external auditors (or both), provided that sufficient budgetary provisions have been provided for.

5.5.3. The ICT Manager together with the two(2) or at least one (1) Senior IT Technicians shall conduct the Internal Audit and make sure that the internal audit action plan against the Audit Findings is accomplished.

5.5.4. The findings of such audits may be included in the audit report to the ICT Steering Committee, or if findings are significant then they must be reported to the Audit and Risk Committee.

5. PHYSICAL CONTROLS

Physical controls with regards to the AbaQulusi Municipality ICT network relate to measures which must be put into place to ensure the physical security and protection of all relevant computer hardware, software, manuals and the computer room. The physical controls are required to provide protection against natural hazards, as well as the risks of theft and/or negligence on the part of AbaQulusi Municipality's officials.

Hardware

6.1.1. Where personal computers have been allocated to officials, such officials shall accept that these computers must be used to fulfil operational functions within the organisation and that their use is restricted to such official functions only.

6.1.2. No hardware may be installed or removed by any municipal official without prior consent and authorisation or direction from the ICT Manager.

6.1.3. No hardware may be removed by any official from municipal premises without the prior written authority of the ICT Manager in consultation with the Municipal Manager. The ICT Manager shall keep such written authority on file, and the official who wishes to remove the relevant hardware must have a copy of such authority for inspection when required.

6.1.4. Any malfunctioning computers must be immediately reported to the IT Helpdesk by the official to whom such equipment has been allocated and the IT Helpdesk shall attend to the required repairs or replacement of the equipment, but subject to the necessary provision having been made in the budget.

6.1.5. Given the significant cost of laser and ink jet printing, officials to whom the use of printers has been allocated must ensure that all printing is kept at a minimum or rather in fast draft print quality. Wherever possible, screen previews should be used rather than physical printing. Original toners and inkjet cartridges must be used when printing is necessary, as not only may the compatible or refilled products void AbaQulusi

Municipality's warranty in respect of the equipment, but they can also (in given circumstances) damage the printers.

Software

6.2.1. The ICT Manager shall maintain a list of approved software to be used on the ICT network, as well as the number of licenses owned and the number of copies of such software loaded onto the system.

6.2.2. Only authorised and licensed software listed on the approved software listing may be loaded onto AbaQulusi Municipality's computers, and this may only be implemented with the consent and supervision of the ICT Manager.

6.2.3. The ICT Manager shall further ensure that this authorised list, referred to as the "Approved Software List", is reviewed and updated periodically in order to address any new software which is released into the market that may be relevant to AbaQulusi Municipality and as the need for new or additional software arises.

Caution: No software may be downloaded through the Internet or via email. Also, pirated software by any official will not be permitted whatsoever.

6.2.4. Standard Applications

6.2.4.1. A new user is entitled but not limited to the following standard applications upon receiving a new computer or the user is new to the municipality:

6.2.4.1.1. Microsoft Office Suite;
6.2.4.1.2. Antivirus Software;
6.2.4.1.3. Munsoft;
6.2.4.1.4. MunAdmin; and
6.2.4.1.5. Acrobat Reader;
6.2.4.1.6. WinZip/WinRar.

6.2.5. Specialised Applications

6.2.5.1. A user is entitled to the following specialised applications once duly authorised:

6.2.5.1.1. Window Outlook Mail;
6.2.5.1.2. Payday;
6.2.5.1.3. Payday T&A;
6.2.5.1.4. MunAdmin;
6.2.5.1.5. Munsoft;
6.2.5.1.6. Contour;
6.2.5.1.7. Truvello;

6.2.5.1.8. Caseware;
6.2.5.1.9. ESS; and
6.2.5.1.10. ArcGIS.

Computer Manuals

6.3.1. The originals of software, hardware, systems manuals and guides shall be kept by the ICT Manager with relevant licenses and discs in the computer room.

6.3.2. The ICT Manager shall further ensure that the manuals and release notes are updated with each new release installed on the systems.

Computer Room

6.4.1. Only the ICT Manager and authorised personnel shall ordinarily have access to the computer room.

6.4.2. The server cabinet and computer room shall be kept locked by the ICT Manager and the keys shall be kept as follows:

6.4.2.1. One set with the ICT Manager;
6.4.2.2. A set of keys is also kept with each ICT staff member;

6.4.3. The ICT Manager shall ensure that adequate fire prevention and extinguisher systems are installed in the computer room, and that this equipment is regularly checked and maintained.

6.4.4. No official may tamper with such equipment, and no official may remove any such equipment from the computer room other than for the purpose of having it tested or serviced.

6.4.5. The ICT Manager shall ensure that a properly designed, maintained and operated air conditioning system is installed in the computer room.

6.4.6. The ICT Manager shall ensure that the servers within the server cabinet are raised (subject to the availability of budget) in the event of flooding.

6.4.7. The ICT department shall regularly test or have tested the Uninterrupted Power Supply (UPS) in order to ensure that it is maintained in an operational condition.

6. ACCESS CONTROL

7.1. GENERAL

7.1.1. Access control is necessary to restrict unauthorised user access to any portion of the IT network or to any particular component of the system. It is therefore necessary that the bona fide user, in order to gain access, must first be authorised, i.e. the access of such user to the system must be properly authenticated.

7.1.2. Access to the IT network comprises three steps:

7.1.2.1. Physical access to a workstation;

7.1.2.2. Access to the system; and

7.1.2.3. Access to specific commands, transactions, programmers and data within the system.

7.2. PHYSICAL ACCESS TO SYSTEMS

7.2.1. After the bona fide user has switched on his or her computer, the user must enter a password to gain further access to systems.

7.3. ACCESS TO SPECIFIC COMMANDS, TRANSACTIONS, PROGRAMS AND DATA WITHIN THE SYSTEM

7.3.1. The ICT Manager shall set access level priorities in accordance with the job descriptions of the officials concerned and to comply with further specific requirements of the officials from the relevant business unit.

7.3.2. Access level and amendment priorities shall be set out in writing by the ICT Manager.

7.4. USER PASSWORDS

7.4.1. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of AbaQulusi Municipality's entire corporate network.

7.4.2. All AbaQulusi Municipality's employees, consultants and temporary staff with access to the organisation's systems are responsible for taking the appropriate steps (as outlined below) to select, maintain and secure their passwords at all times and never use an account assigned to another user, as they will be held responsible for total use or misuse of their account.

7.4.3. All officials, to whom user passwords have been allocated, must ensure that these passwords are properly safeguarded.

7.4.4. Under no circumstances may the employee share any user password with colleagues.

7.4.5. Passwords are used for various purposes at AbaQulusi Municipality. Some of the more common uses include: user level accounts, web accounts, email accounts, screensaver protection, application logins and logins to IT Hardware.

7.4.6. All users should be aware of how to select strong passwords. Hence, the following password guidelines must be adhered to by all users on all servers and computers within AbaQulusi Municipality:

7.4.6.1. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

7.4.6.2. Passwords must not be inserted into email messages or other forms of electronic communication.

7.4.6.3. Passwords should not be a word in any language, slang, dialect or jargon.

7.4.6.4. Do not use the same password for AbaQulusi Municipality accounts as for other non-organisational access (e.g. personal account, option trading, benefits, etc.).

7.4.6.5. Users must not use the "Remember Password" feature for applications (e.g. Internet Explorer, etc.), and must not write passwords down.

7.4.6.6. Users must not store passwords in a file on any computer system (including laptops or similar devices).

7.4.6.7. Users must avoid using the same password for multiple applications.

7.4.6.8. If an account or password is suspected to have been compromised, the user must report the incident to the IT Helpdesk and change all their passwords accordingly.

7.4.6.9. If a user is requested to provide their password details to any IT staff member, they must ensure that they monitor the actions performed by the staff member. Thereafter, the user should change their password immediately once the IT staff member has left.

7.4.6.10. Where possible, systems have been configured to follow AbaQulusi Municipality standards. The organisation's requirements for password settings should be as follows:

7.4.6.10.1. A minimum of eight (8) characters in length;

7.4.6.10.2. Must be changed every 30 days;

7.4.6.10.3. A password history of (twenty-four) 24 generations should be maintained.

7.4.6.10.4. User accounts are set to lockout after 3 unsuccessful login attempts; and

7.4.6.10.5. Users should not use their usernames as passwords;

7.4.6.11. Additional configuration settings for Active Directory Server

7.4.6.11.1. A minimum password age of 1 day;

7.4.6.11.2. Accounts should be set to lockout indefinitely (until the ICT Manager unlocks);

7.4.6.11.3. Accounts are set to lockout after 3 invalid log-on attempts.

- Users must take note that for all activity performed using their user name and password, they will be held accountable and may face disciplinary action in the event of misuse.
- It is therefore of utmost importance that users follow the guidelines below on password construction and safeguarding their password in order to minimise the threat of others obtaining their passwords.

7.4.8.1. Personal details, such as spouse's name, license plate, ID number or birthday, must not be used.

7.4.8.2. Words in a dictionary, derivatives of user ID's and common character sequences such as "123456" must not be used as well.

7.4.8.3. Passwords should not be based upon month / year combinations such as "jan09" or "april2009". Hackers use these types of words in attempts to guess passwords.

7.4.8.4. Users must not use cyclical passwords. For example, users should not add a numeric at the end of the password in sequence.

7.4.8.5. Passwords must not consist of all identical numeric or alphabetic characters, such as: "1111111" or "aaaaaaa".

7.4.8.6. Employees must never share their passwords with anyone, including ICT staff, administrative assistants or secretaries.

7.4.8.7. All passwords are to be treated as sensitive organisational information.

7.4.9. Users must take note of and adhere to the following "Don'ts":

7.4.9.1. Do not reveal a password over the phone to anyone.

7.4.9.2. Do not reveal a password in an email message.

7.4.9.3. Do not talk about a password in front of others.

7.4.9.4. Do not hint at the format of a password (e.g. "my family name").

7.4.9.5. Do not reveal a password on questionnaires or security forms.

7.4.9.6. Do not share a password with family members or colleagues.

7.4.9.7. Do not reveal a password to co-workers while on vacation.

7. DATA SECURITY CONTROL

8.1. PRIVILEGES AND EXPOSURE

8.1.1. Access by users to AbaQulusi Municipality's IT systems shall be restricted in accordance with the job descriptions of officials concerned.

8.1.2. Users are responsible for the protection of sensitive information by ensuring that only officials whose duties require such information are allowed to obtain knowledge of such information while it is being processed, stored or in transit.

8.2. BACKUPS

8.2.1. Backup procedures will be determined by the ICT Manager and communicated to all relevant users accordingly.

8.2.2. Backup procedures shall be adhered to by all users on the system.

8.2.3. Backups will be stored in a secure site.

8. INTERNET AND EMAIL

9.1. USE OF INTERNET

9.1.1. Internet access and related IT resources are provided to AbaQulusi Municipality at significant cost and are made available primarily for business use.

9.1.2. Users who have access to the Internet shall use this access solely in connection with official responsibilities, including communicating with clients, working related partners, local and provincial government agencies, providers of goods and services to AbaQulusi Municipality, and to also research relevant topics and obtain business related information which is of use to AbaQulusi Municipality.

9.1.3. Limited personal use on approved sites may be authorised when such access will be to the best advantage of AbaQulusi Municipality only.

9.1.4. All users who have access to the Internet shall conduct themselves honestly and appropriately, and respect copyrights, software licensing rules, property rights, privacy and the prerogatives of others.

9.1.5. Officials who use the Internet shall ensure that intellectual property of others is protected and that AbaQulusi Municipality's resources are not misused, that information and data security (including confidentiality where applicable) are at times respected, and that the Internet is not used for any form of abuse.

9.1.6. Every official using the Internet facilities of AbaQulusi Municipality shall identify himself or herself honestly, accurately and completely.

9.1.7. Officials using the Internet shall do so only when this is required to fulfil their official responsibilities and/or when they are authorised to do so.

9.1.8. Whenever an official downloads any file from the Internet, such a file must be scanned for viruses before it is run or accessed. If the official is uncertain as to the procedure to be followed, such official shall immediately seek assistance of the IT Helpdesk.

9.2. AUTHORITY TO SPEAK ON THE BEHALF OF ABAQULUSI MUNICIPALITY

9.2.1. Only those officials who are duly authorised by the Municipal Manager to speak to the media, to analysts, in public gatherings or send external emails on behalf of AbaQulusi Municipality may do so.

9.3. INTEGRITY OF ABAQULUSI MUNICIPALITY'S IMAGE

9.3.1. Officials who are authorised to speak on behalf of AbaQulusi Municipality, as set out in section 9.2 above, shall ensure that they honour the image and integrity of AbaQulusi Municipality at all times, do not engage in any unauthorised political advocacy, and refrain from the unauthorised endorsement by AbaQulusi Municipality of any commercial product or service not sold or provided by AbaQulusi Municipality itself.

9.3.2. Officials must ensure that, where inputs are provided on behalf of AbaQulusi Municipality to any news group or chat room, such inputs have been grammar and spell-checked, and that the inputs reflect the view of AbaQulusi Municipality (where applicable) rather than the personal opinions of the writer.

9.4. SECURITY

9.4.1. Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, Internet address screening programmed or any

other security systems installed by the ICT Manager or any IT suppliers to assure the safety and security of AbaQulusi Municipality IT network.

9.4.2. Any officials who obtains a password, which allows access to the Internet and/or the organisation's IT network, shall keep such a password confidential, except if any occasion arises where any authorised technical support official requires knowledge of such password in order to solve a computer related problem.

9.4.3. As set out in 7.4 above, the present policy strictly prohibits the sharing of passwords between employees.

9.4.4. Logging onto the IT network or Internet with one's personal password, and then allowing another user to use or work on the Internet or the IT network, shall be viewed as an attempt to bypass official security procedure, and is strictly prohibited and will be dealt with accordingly.

9.4.5. Every authorised user shall sign all ICT Security Policy Compliance Agreements provided to them by the ICT Manager before attempting to gain access to the Internet and/or the network.

9.4.6. The ICT Manager will review all Internet activities and analyse the relevant usage patterns. Thereafter, appropriate action will be taken on the user wherever any abuse of the system is evident.

9.5. ELECTRONIC MAIL (EMAIL)

9.5.1. Only authorised officials shall use the available email facility.

9.5.2. The ICT Managershall scan all emails for any inappropriate content or offending words or phrases.

9.5.3. All copies of emails shall be kept as records.

9.5.4. Only authorised officials shall be permitted to receive attachments through the email system.

9.5.5. The ICT Manager shall maintain a list of prohibited and blocked email, and shall update and amend such list as circumstances require.

9.6. INTERNET BROWSER

9.6.1. As indicated in sections 9.4 and 9.5 above, AbaQulusi Municipality reserves the right to block and track all visited sites.

9.7. UNACCEPTABLE PRACTICES

9.7.1. No official may display any kind of sexually explicit material on any organisational system. Furthermore, no sexually explicit material may be archived, stored, distributed, edited or recorded using any of AbaQulusi Municipality's resources.

9.7.2. The ICT Manager shall have the right to block access from within AbaQulusi Municipality's networks to all Internet sites identified as inappropriate. If any user is connected to a site which contains sexually explicit or otherwise offensive material, such user must immediately disconnect from the site concerned.

9.7.3. AbaQulusi Municipality's IT related facilities, and especially its Internet facilities, may not be used knowingly by any official to violate the laws and regulation of the Republic of South Africa or any other nation, or the laws and regulations of any province or municipality.

9.7.4. The use of any municipal resources or illegal activities shall be grounds for the immediate dismissal of the official concerned, and the Council and it's officials undertake further to cooperate with any legitimate law enforcement agency in this regard.

9.7.5. No employee may knowingly use AbaQulusi Municipality's IT facilities and resources to download or distribute pirated software or data.

9.7.6. No official may knowingly use the Internet facilities to propagate any viruses, worms, Trojan horses or trap doors (i.e. malicious code).

9.7.7. No official may knowingly useAbaQulusi Municipality's Internet facilities to disable or overload any computer or network or to circumvent any system intended to protect the privacy or security of another user.

9.7.8. No employee with authorised Internet access may upload any software licensed to AbaQulusi Municipality or data owned or licensed to AbaQulusi Municipality without prior authorisation of the ICT Manager.

9.7.9. No official may create a communication link requiring dial-out access from any computer which is also connected to the IT network.

9.7.10. No official may use any software which is not provided or approved by the ICT Manger.

9.7.11. Only the ICT shall authorise the provision of email addresses to authorised users.

9.8. OWNERSHIP AND CLASSIFICATION OF DATA

9.8.1. Any AbaQulusi Municipality data that is created, sent, printed, received or stored on systems owned, leased, administered or authorised by AbaQulusi Municipality is the property of AbaQulusi Municipality and its protection is the responsibility of AbaQulusi Municipality's designated custodians and users.

9.8.2. No Official is allowed to Purge Municipal Information, temper with admin password especially during leave of absence or resignation, remotely connect on Municipal Local Area Network nor claim to have ownership on which ever data or information thereof, no deletion of information is allowed after an employee had resigned, left for another position and even in a case of dismissal , therefore should any one commit such crime it can lead to disciplinary and that employee can even reported to the Law Enforcement and even be arrested for such offence.

9.8.3. Data shall be classified as either: Confidential, Sensitive or Public.

9.8.4. **Confidential:** Sensitive data that must be protected from unauthorised disclosure or public release based on local or governmental law (e.g. the Promotion of Access to Information Act, No. 2 of 2000)and other constitutional, statutory, judicial and legal agreements.

- Examples of "Confidential" data may include but are not limited to:

9.8.3.1.1. Personally Identifiable Information, such as a name in combination with Identification Number (ID) and/or financial account numbers

9.8.3.1.2. Employee records

9.8.3.1.3. Intellectual Property, such as copyrights, patents and trade secrets

9.8.4. **Sensitive:** Sensitive data that may be subject to disclosure or release under the Promotion of Access to Information Act, No. 2 of 2000, but requires additional levels of protection. Examples of "Sensitive" data may include but are not limited to:

9.8.4.1.1. Operational information

9.8.4.1.2. Personnel records

9.8.4.1.3. Information security procedures

9.8.4.1.4. Research

9.8.4.1.5. Internal communications

9.8.5. **Public:** Information intended or required for public release as described in the Promotion of Access to Information Act, No. 2 of 2000. However, any data owned or under the control of the South African Government must comply with the national classification authority and national protection requirements.

9.8.6. Authorised officials who don't participate in Internet chats and news groups shall refrain from revealing confidential municipal information, client data and any other material covered by existing council policies and municipal procedures with regards to confidential information.

9.8.7. Officials, who release protected information through the Internet whether or not it is inadvertent, shall be subject to all the applicable penalties in terms of AbaQulusi Municipality's existing data security policies and procedures.

9. WIRELESS SECURITY

10.1. All wireless Access Points / Base Stations connected to the AbaQulusi Municipality network must be registered and approved by the ICT Manager.

10.2. Access Points / Base Stations must be subject to periodic penetration tests and audits.

10.3. All wireless Network Interface Cards (i.e., PC cards) used in laptop or desktop computers must be registered with the ICT Manager.

10.4. All access points (APs) must be logically secured to prevent unauthorised access to the AP configuration environment. T

10.5. AP devices must be configured to only allow pre-defined authorised administrators to make configuration changes.

10.6. AP's must be physically secured to protect the AP against physical manipulation.

10.7. All wireless LAN access must use AbaQulusi Municipality approved vendor products and security configurations.

10.8. All computers with wireless LAN devices must utilise an AbaQulusi Municipality approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic.

10.9. Wireless implementations must maintain point to point hardware encryption of at least 56 bits.

10.10. Wireless implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.

10.11. Wireless implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

10.12. The SSID shall be configured so that it does not contain any identifying information about the AbaQulusi Municipality, such as the AbaQulusi Municipality, division title, employee name, or product identifier.

10. OFFICIAL WEBSITE

11.1.1. The ICT Manager shall be responsible for the maintenance of AbaQulusi Municipality's website.

11.1.2. Each Head of Department shall ensure that all information required by the Municipal Finance Management Act, as well as any other relevant legislation and Council Policies, is promptly and appropriately submitted to the ICT Manager for display on the official website.

11.1.3. The ICT Manager shall (in consultation with the relevant Heads of Department) further decide on any other information to be made available on the website.

11.1.4. Only the ICT Manager shall be authorised to amend, add and delete information on the official AbaQulusi Municipality website.

11. PROTOCOLS

12.1. Reporting Security Incidents

12.1.1. If an IT Security incident or breach is suspected or noticed by any employee, then it is the obligation of that employee to immediately notify the ICT Manager.

12.1.2. Users are required to note and report any suspected security threats and/or weaknesses in and around IT systems and services.

12.1.3. Critically, users must not attempt to prove a suspected weakness within a system, as testing weaknesses might be interpreted as a potential misuse of the system, which could lead to disciplinary action thereafter.

12.1.4. The ICT Manager is tasked with the security responsibility of AbaQulusi Municipality and must report all instances of a breach of security, or failure to comply with security measures, or conduct constituting a security risk, as soon as possible to the Chief Directorate Security of the National Intelligence Agency (NIA), and where appropriate to the South African Police Services (SAPS - Crime Prevention Unit) or the South African National Defence Force (SANDF - MI). Where official encryption is concerned, a security breach must also be reported to the South African Communication Security Agency (SACSA).

12.1.5. When a breach of security occurs, the existing channels must be used to report it. It is the responsibility of the ICT Manager to ensure that all breaches of security are reported.

12.2. User Names

12.2.1. All users must have proper usernames and passwords that will grant them access to the network and network services available for AbaQulusi Municipality.

12.2.2. The username and password must be in accordance with the following standards:

12.2.2.1. Minimum length: 8 characters

12.2.2.2. Maximum age: 30 days

12.2.2.3. Composition: Alphanumeric. Special characters are optional

12.2.2.4. Password history: 24 generations should be maintained

12.2.2.5. The screensaver setting should be set to 5 minutes of inactivity.

12.2.2.6. User accounts will be locked automatically if the user enters the incorrect password on 3 consecutive occasions.

12.2.3. As such, this standard incorporates the user's first letter of user's full name and user's full surname for the Network and all systems (e.g. Joe Blogg's ID would be: jblogg)

12.2.4. In the case of duplicate user names, the user's name will be placed vice versa of the above to make a user ID unique.

12. PC SUPPORT

13.1. All support must be performed against a logged call to the IT Helpdesk with the details of the call that was logged.

13.2. All network and PC support calls should be given priority and should be attended to as soon as is possible.

13. DISASTER RECOVERY PLAN

14.1. The ICT Manager, in consultation with the Director of Corporate Services and with the approval of Council, shall enter into such agreements with AbaQulusi Municipality's IT suppliers and/or with one or more other municipalities as necessary to ensure that the AbaQulusi Municipality Disaster Recovery Plan is in place, is operational, and is reviewed and tested at least once a year.

14.2. The ICT Manager shall prepare, review and update (as circumstances require) a list of persons who must be contacted by users in the event of any disastrous occurrence as set out in the AbaQulusi Municipality Disaster Recovery Plan.

14.3. Such lists shall be made available to all authorised users on AbaQulusi Municipality's ICT Network.

14. TRAINING

15.1. The AbaQulusi Municipality has a Training section within the Corporate Services Department that is responsible for the selection and training of employees.

15.2. The Training section shall coordinate, and where possible, shall provide the appropriate training to such officials as deemed necessary.

15. ACCEPTANCE OF AND COMPLIANCE WITH THE ICT SECURITY POLICY

16.1. Every employee who is allocated the use of any AbaQulusi Municipality IT equipment and/or authorised to access the Internet and/or AbaQulusi Municipality's computer network shall be provided with an email copy of the ICT Security Policy by the ICT Manager.

16.2. All employees are required to read through the entire ICT Security Policy and then sign the ICT Security Compliance Agreement form (see Appendix A) attached to the policy in order to indicate that they have read, understood and accept to comply with this policy accordingly.

16. ENFORCEMENT

Non-compliance, violation and disregard of this policy by any AbaQulusi Municipality employees, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual's employment contract, depending on the circumstance and the gravity of the transgression. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the individual and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the individual.

17. APPENDICES

ICT Security Policy Compliance Agreement

Appendix A

ICT Security Policy Compliance Agreement

Employee Name (PRINTED):

_____

Department:

_____

I agree to take all reasonable precautions to assure that municipal internal information, or information that has been entrusted to the AbaQulusi Municipality by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with AbaQulusi Municipality, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Municipal Manager, who is the designated Information Owner.

I have access to an emailed copy of the AbaQulusi Municipality ICT Security Policy, I have read and understood this policy, and I understand how it impacts on my job. As a condition of continued employment, I agree to abide by the policy and other municipal requirements, including non-disclosure of municipal information. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of ICT policies and procedures to the designated ICT Manager in charge.

Employee Signature: **Date:**

_____ _____

ICT Manager Signature: **Date:**

_____ _____

INFORMATION COMMUNICATION AND TECHNOLOGY STRATEGY

Table of Contents

1 INTRODUCTION

In the modern business world ICT has become a strategic imperative without which organisations cannot survive. Due to this and other factors, ICT strategic planning has become critical for every organisation. This document aims to provide direction to AbaQulusi Municipality for a 3 to 5 year planning horizon but is a living document and will change as the operating environment of the municipality changes.

2 PURPOSE

The purpose of developing an ICT Strategy is as follows:

- Ensure ICT's alignment with the municipality's strategy;
- Enabling of strategic opportunities;
- Revision of outdated applications and facilitate the improvement of key business processes where possible;
- Elimination of 'islands of information' via the establishment of integrated or connected systems which allow information sharing betweendepartments;
- Review of infrastructure to ensure that networks and servers cater for current and future needs;
- The ICT Strategy will also take into consideration relevant industry trends and incorporate applicable IT best practices.

3 MUNICIPAL VISION

In terms of the above statement, the ICT Department is committed in supporting initiatives embarked on by the municipality to achieve the vision.

4 MUNICIPAL MISSION STATEMENT

To be the progressive, prosperous and sustainable economic hub of Zululand

The ICT Department supports and will work with the various internal business units in the municipality to achieve the vision and mission statement as set out in the IDP.

5 Current ICT Environment

5.1. As-is Assessment

The current ICT Landscape contains the following Applications:

Application	Processes relying on Application
MunAdmin	Electronic Document Management
MunSoft	Financial System (ERP)
Payday	Payroll HR
TCS	Traffic - Fines, Court rolls
ESS	Leave
Payday T&A	Time and Attendance
Contour	Pre-paid Electricity
Webmin	Firewall
ArcGIS	Town Planning, Spatial mapping
Caseware	Financial Reporting Tool

5.2. Sites

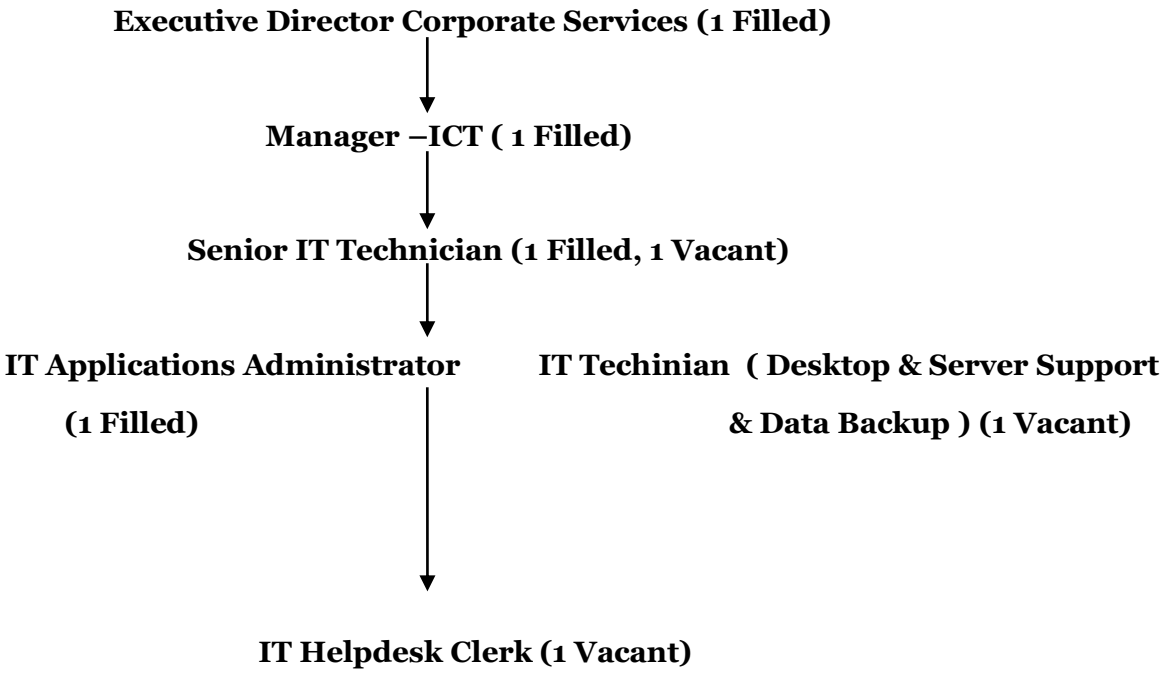
AbaQulusi Municipality's IT Networks are linked to the following sites:

LIST ALL SITES

- **Museum**
- **Public Safety**
- **Technical Services**
- **Community Services**
- **Corporate Services**
- **eMondlo Municipality**
- **Corronation**
- **Hlobane**
- **Licensing**
- **Louwsberg**

5.3. Reporting Structure of ICT

The reporting structure for IT is as follows:



5.4. Services Providers

The following services providers have been engaged by AbaQulusi Municipality:

Service Providers	Location	Services
MunComp	Based in Gauteng	Electronic Document Management
MunSoft	Based in Gauteng	Financial System (ERP)
Payday	Based in Gauteng	a. Payroll HR b. Leave c. Time and Attendance
TCS	Based in Gauteng	Traffic - Fines, Court rolls
Contour	Based in Durban	Pre-paid Electricity
DC Data	Based in Pietermaritzburg	Firewall

6 Alignment of ICT strategy to idp

The table below is a representation of how ICT will support the municipality in achieving objectives set out in the IDP

Business Strategy Objective	Related ICT Strategy Objective
To reduce levels of infrastructure backlogs by providing Basic Services, Facilities and maintaining existing infrastructure.	To ensure employees have the tools of trade ie; desktop computers and/or relevant software systems are up to date, and the hardware is upgraded, thus ensuring minimal downtime.
Empower and capacitate institutional structures and promotion of transparent cooperative governance.	Development of IntraNet to provide basic information on Email and Internet security standards for users and provide a central communication tool internally for users to manage communications between departments.
Ensure sound financial management and accountability.	Development and monitoring of ICT infrastructure and relevant security mechanisms with provision of reports.
Ensure transparency, accountability and community involvement in municipal affairs.	Updating, and upgrading of website and Upgrading to newer technologies. Updating/Upgrading to newer software as part of the new technology drive forward and use of website as one of the many available communication tools with the public.

7 Issues arising

Based on our interviews with senior management the following points were highlighted as issues within the business. The validity of the points below was not tested but represent the views of individuals interviewed:

Ref	Process/Activity	Problem
1	IT Security Issues Related to users	Users should be workshopped on the IT Policy.
3	Disaster Recovery Server Room	A backup server room and/or disaster recovery should be maintained offsite.
4	Response times for IT related problems	Response times of technical staff are inadequate. This is due to lack of staff.
5	Help Desk Management	Calls are not logged correctly with the Help Desk which results in problems not being resolved on time, which also additionally contributes to response times.
8	Network Speed	Some users have experienced slow network response times, often contributing factors are devices that have not been cleaned or checked for any viruses/worms/Trojans/malware and others has been used in a business desktop workstation, of this includes mobile phones.
9	IT Security and Governance	There is low focus on IT Security and Governance within the municipal executive management.

8 Migration Strategy to Future ICT Environment

Strategic ICT Initiatives

Based on the information gathered and research performed, the following initiatives need to be implemented to assist AbaQulusi Municipality in achieving their business objectives going forward:

8.1.1. IT Staff Training
8.1.2. Security Awareness Training
8.1.3. Establish Service Level Agreement management
8.1.4. Server Room Upgrade and expansion with backup server room
8.1.5. System Improvements
8.1.6. Monitoring systems.

ICT Implementation Plan

	2018	2019	2020	2021	2022
IT Staff Training					
Security Awareness Training					
Establish Service Level Agreements					
Backup/Server Room Upgrade					
System Improvements & Expansion					
Business Continuity					

Detailed ICT Initiatives Details

TRAINING INITIATIVE

8.3.1. IT STAFF TRAINING

The objective of this initiative is for the ICT Manager & Senior Technician to attend IT skills Enhancement and Training, which will be split over the next two financial years.

The ICT Manager will attend the following Training programmes:

- Microsoft Certified IT Professional (MCITP) – from September 2014 and will take 8 months to complete.
- Information Technology Infrastructure Library (ITIL) from March 2016 and will take 6 Months to complete.

The Senior IT Technician will attend the following Training programmes:

- Cisco Certified Network Associate (CCNA) – from March 2014 and will take 8 months to complete.
- Information Technology Infrastructure Library (ITIL) from March 2015 and will take 6 Months to complete.

8.3.2. SECURITY AWARENESS TRAINING

The objective of this initiative is to make all employee of the municipality aware of the security controls and policies in place.

The ICT Department/Section will conduct security awareness training sessions with all employees once the policies have been approved by Council and these will be performed every 6 months if the ICT Department/Section is able to do so.

8.3.3. SERVER ROOM UPGRADE

The objective of this initiative is to improve and enhance all environmental and physical controls in the server room and the Technical Support Offices.

The duration of this initiative will be 3 years once the budget has been approved.

The following are some of the controls that will be put in place:

- Fire detection and Fire Extinguishers – handheld fire suppression – Servicing and/or replacements.
- Conceal window area in the server room
- New equipment – racks, servers and cabinets

9 Review periods

This ICT Strategy document will be reviewed on a yearly basis. The impact of the strategy / progress towards the attainment of goals will be monitored on a quarterly to bi-annual basis.

PATCH MANAGEMENT POLICY

TABLE OF CONTENTS

32. OVERVIEW

This Policy establishes certain requirements which must be met by all computers connected to AbaQulusi Municipality network to provide the AbaQulusi Municipality with a trusted and secure network infrastructure to support the effective delivery of IT resources and mechanisms to help the organisation realise its goals and objectives in maintaining a secure IT environment. It attempts to set standards in terms of patch management.

33. PURPOSE

It is the ICT Department's responsibility to ensure that all computer devices (including servers and desktops) that are connected to the AbaQulusi Municipality network have the latest security patches installed. This document describes the management of IT Security/Integrity Patches for the AbaQulusi Municipality. This document provides a common definition of what is required when performing Security Patch Management activities for the AbaQulusi Municipality.

34. SCOPE

The scope for this process comprises the following:

- IT Security/Integrity Patches, which includes Security Updates and Hot Fixes.
- Systems/Platforms, Middleware and Applications.
- All software on all platforms and devices.

35. DEFINITIONS

Patches - typically released to protect against known exploits in operating system or application code or to address functionality issues or a new vulnerability.

Vulnerabilities - weaknesses in software that can be exploited by an entity to gain elevated privileges is authorised to have on a computer or system. Not all vulnerabilities have related patches. These situations require workarounds to attempt to mitigate “un-patched” vulnerabilities.

Threats - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

CERT - CERT is the Internet's official emergency team. CERT focuses on security breach and incidents, providing alerts and incident-handling and avoidance guidelines. CERT also

conducts an ongoing public awareness campaign and engages in research aimed at improving security systems.

36. GENERAL POLICY

5.1. Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, approval, installing and verifying.

5.2. AbaQulusi Municipality is committed to complying with applicable compliance laws, rules and standards.

37. PATCH MANAGEMENT

6.6. ICT RESPONSIBILITIES

6.1.1. The ICT Manager must ensure that all ICT systems are patched in timely manner as laid out in this policy.

6.1.2. The ICT Manager must review current threats and vulnerabilities and to check relevant advisories to monitor any potential threats or vulnerabilities.

6.1.3. The ICT Manager must establish and implement a departmental program for patch management on all ICT systems.

6.1.4. The ICT Manager must ensure that all ICT staff members are made aware of this policy and relevant procedures.

6.1.5. The ICT Manager is responsible for assigning other authorised personnel specific patch management and vulnerability correction responsibilities.

6.1.6. The ICT Manager must ensure that a departmental inventory of hardware and software patch status is developed to maintain and track the status of all patch actions and vulnerability corrections and to provide rapid response to internal or external reporting requirements.

6.1.7. A Patch Management Compliance form (see Appendix B) must be completed by the ICT Manger for all patches installed.

6.1.8. The ICT Manager must report the patch management status of the municipality on a monthly basis to the Director Corporate Services using the Patch Management Compliance Form.

6.1.9. The ICT Manager must act as a Point of Contact (POC) for information security to provide guidance and assistance to individuals designated patch management responsibilities.

6.1.10. The ICT Manager must develop and publish policy and procedural guidance on patch management.

6.1.11. The ICT Manager must monitor patch management on a municipal-wide basis.

6.7. ALL STAFF & THIRD PARTIES

6.2.1. It is the responsibility of each user, both individually and within the municipality, to ensure prudent and responsible use of computing and network resources.

6.2.2. End Users must report any suspected lack of compliance with this policy to the ICT Manager. Failure to do so constitutes a violation of this policy.

6.8. THE MUNICIPALITY

6.3.1. Reserves the right to monitor for violations of this policy.

6.9. MONITORING

6.4.1. The ICT Manager will monitor and/or subscribe to security mailing lists, review vendor notifications and web sites and research specific public web sites for the release of new patches.

6.4.2. Monitoring will include, but not be limited to, the following:

6.4.2.1. Scanning the AbaQulusi Municipality's' network to identify known vulnerabilities.

6.4.2.2. Monitoring Computer Emergency Readiness Team, CERT, other advisories and websites of all vendors that have hardware or software operating on the municipality's network.

6.4.2.3. Where a vendor has no subscription service available for the notification of patches that are released, the ICT Manager will perform manual monitoring at least monthly.

6.10. ASSESSING AND CLASSIFYING RISK

6.5.1. Once alerted to a new patch, the ICT Manager will download and review the new patch.

6.5.2. The ICT Manager will assess the security patch for risk and severity and assign a classification.

6.5.3. The ICT Manager will categorise the criticality of the patch according to the following:

6.5.3.1. Emergency - an imminent threat to the AbaQulusi Municipality's' network.

High - A vulnerability whose exploitation could allow the propagation of malicious software without user action.
A vulnerability whose exploitation could result in compromise of the confidentiality, integrity or availability of user's data or of the integrity or availability of processing resources.

Medium - Exploitability is mitigated to a significant degree by factors such as default configuration, auditing or difficulty of exploitation.

6.5.3.2. Low - A vulnerability whose exploitation is extremely difficult or whose impact is minimal

6.11. TESTING

6.6.1. The ICT Manager will assess the effect of a patch to the municipality's' infrastructure prior to its deployment.

6.6.2. The ICT Manager will also assess the affected patch for criticality relevant to each platform (e.g., servers and desktops).

6.6.3. All patches will undergo testing for each affected platform before release for implementation.

6.6.4. If the ICT Manager categorises a patch as an Emergency, it is considered an imminent threat to AbaQulusi Municipality's' network. Therefore, the AbaQulusi Municipality assumes greater risk by not implementing the patch than waiting to test it before implementing.

6.6.5. Once the ICT Manager is satisfied that the implementation of a new patch will not cause any unexpected behaviour, he must agree upon a schedule for implementation.

6.6.6. It is the responsibility of application end users to identify any problem(s) with a patch or patches and to notify the ICT Manager of the problem(s) post installation.

6.12. AUTHORISATION AND NOTIFICATION

6.7.1. Regardless of criticality, each patch requires the creation and approval of a request for change prior to implementing the patch.

6.7.2. The ICT Manager will obtain authorisation for implementing Emergency patches via an emergency change and obtain the Director Corporate Services approval.

6.7.3. The ICT Manager will implement patches during regularly scheduled maintenance (downtime) periods.

6.7.4. The Director Corporate Services must approve the patch schedule prior to implementation.

6.7.5. For new network devices and servers, each platform will follow established hardening procedures to ensure the installation of the most recent patches.

6.7.6. Since a security patch may cause a system to malfunction, the ICT Manager should proactively announce the implementation of a patch or patches.

6.13. IMPLEMENTATION

6.8.1. The ICT Manager will implement Emergency patches within eight hours of availability. As Emergency patches pose an imminent threat to the network, the implementation may precede testing.

6.8.2. In all instances, the ICT Manager will perform testing pre-implementation and document it for auditing and tracking purposes.

6.8.3. The ICT Manager will obtain authorisation for implementing Emergency patches via an emergency change (Refer to the ICT Change Management Procedure).

6.8.4. The ICT Manager will implement High, Medium and Low patches during regularly scheduled maintenance (downtime) windows. Each patch will have an approved change record.

6.8.5. Patches will be implemented on all devices according to the timeframes below:

Criticality of Patch	Timeframe to Implement
Emergency	Within 8 hours of availability
High	Within 30 days of availability
Medium	Within 60 days of availability
Low	Within 90 days of availability

6.14. VERIFICATION

6.9.1. Following the implementation of all patches, the ICT Manager will verify the successful installation of the patch and that there have been no adverse effects.

38. HOT FIXES

7.1. Operating system updates, hotfixes and service packs will only be installed under the following conditions:

7.1.1. If a specific issue has been identified that requires the installation of the update, hotfix or service pack.

7.1.2. All relevant documentation for the update, hotfix or service pack has been reviewed to determine any configuration changes and potential problems that may be introduced and to determine whether all requirements for installation are being met.

7.1.3. The update, hotfix or service pack has been installed and tested in a test environment to determine any possible issues that may result in the production environment.

7.1.4. It has been established that there is a greater risk in not applying the update, hotfix or service pack then there is in the risk of applying it.

7.1.5. Approval for installation of the update, hotfix or service pack has been obtained from the Director Corporate Services.

39. ENFORCEMENT

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

40. APPENDICES

9.1. Appendix A - Patch Control Form

9.2. Appendix B - Monthly Patch Management Compliance Form

APPENDIX A - PATCH CONTROL FORM

PATCH INFORMATION:			
Patch Source or Vendor Name (if Patch was alerted to municipality by system vendor):		Email:	
Date Requested:		Contact No.:	
Signature:		Office:	
System Affected:		Patch Request No:	
DESCRIPTION OF PATCH		Risk Rating:	
BUSINESS JUSTIFICATION			
NATURE AND PRIORITY			

AUTHORISATION AND APPROVAL				
	Name	**Title**	**Date**	**Signature**
Approved by:				
Authorised by:				
TESTING OF CHANGES	Testing Required : YES / NO If "NO", provide reason for not testing: _____ Testing Documentation/Screen Prints – Attached to Change Request: YES / NO			

SIGN-OFF COMPLETION OF CHANGE				
	Name	**Title**	**Date**	**Signature**
Tested by (where applicable):				
Patch Implemented by:				

APPENDIX B - PATCH MANAGEMENT COMPLIANCE FORM

Patch Request Number:	Details of Change:	Change Documentation Attached:	Change Management Process Followed: (Yes/No)	Details of Exceptions Noted:
Checked by:				
Designation:				
Sign:				
Date:				

ICT PERFORMANCE AND CAPACITY MANAGEMENT POLICY

Table of Contents

1. INTRODUCTION

This policy applies to all employees of AbaQulusi Municipality and all parties that interact with the information and systems of the Municipality.

The purpose of this document is to detail the correct performance and capacity management procedure that is to be followed for system and application utilised.

2. Policy Statement

AbaQulusi Municipalitymust define the functions and processes for technical support of infrastructure and/or applications, as well as IT operational control of day-to-day activities and tasks.

The objective of this policy is to ensure that the IT operational environment is well maintained to achieve stability of day-to-day processes and activities

All IT equipment must be monitored regularly and a uniform process for performance and capacity management must be established at AbaQulusi Municipality. Equipment used to run key applications should be monitored more regularly.

3. Roles and Responsibilities

ICT Manager:

Ensures that operational policy and procedure documents are continuously updated.

Monitors compliance to the policy, and is accountable for ensuring that IT operations staff carries out the appropriate operational tasks.

Accountable for ensuring that the Municipality's ICT Operations are well managed and provide for a stable IT environment.

Responsible for carrying out operational duties to achieve stability of the operational environment.

Users

A user of information has the responsibility to:

- Use the information only for the purpose intended;
- Comply with all controls established by the municipality;
- Ensure that classified or sensitive information is not disclosed to anyone without permission; and
- Ensure that his/her individual passwords and/or physical access controls are not disclosed to, or used by anybody else.

4. IT Operations management

4.1. A stable IT infrastructure must be designed and maintained. The following areas must be managed at a minimum:

- Server environments
- Networks
- Storage and archiving
- Databases
- Desktops
- Backups

4.2. The execution of operational activities and events in the IT infrastructure must include audit logging and monitoring.

5. Server Configuration policy

5.1. Server equipment must be documented and the following information must be maintained at a minimum:

- Host contact information and location of server equipment
- Sever hardware and operating system version and serial numbers
- Server equipment purpose/function and applications
- Password groups for privileged passwords
- Configuration information (server name, IP Address, and application specific information)

5.2. Passwords on server equipment must be maintained in accordance with the Municipality's ICT Security Policy, at least two(2) Senior IT Technicians should share responsibilities of network and server administration.

5.3. Any changes to existing server equipment must follow the Municipality's Change Management Policy/Procedures and be reviewed by the ICT Manager.

5.4. Server equipment and operating systems must only be installed by an approved source, ICT Manager and the Two(2) Senior IT Technicians or at least one(1) and the delegated and Trained IT Technician with server related credentials or experience to ensure the business continuity. Server equipment must operate with only licensed versions of the operating system and software.

5.5. All critical and security related patches/hot-fixes released by vendor(s) must be installed. This must be installed in accordance with the Municipality's Patch Management Policy and Procedure. This applies to all services installed on the server equipment, even though those services Patch Management Policy may be temporarily or permanently disabled.

5.6. IT must have controlled processes in place to ensure the municipality's server environment/equipment remains current with appropriate patches/hot-fixes.

5.7. All services and applications that are unused or not serving business requirements must be disabled except where approved by the ICT Manager.

5.8. Remote system administration (through privileged access) must be conducted using approved VPN secure solutions in accordance with the municipality's ICT Security Policy.

5.9. All system, application and security related events on server equipment must be logged with log files archived. Archival of server event logs must meet the following minimum (or better where compliance with specific legislation is required) practice:

- All server event logs must be kept online for minimum of one week;
- Daily backups of event logs must be retained for at least one month;
- Weekly backups of event logs must be retained for at least one month; and
- Monthly backups of event logs must be retained for a minimum of two years.

5.10. The ICT Manager must review the Daily Operations Tasks Checklist (Appendix A) and the Monthly Performance and Capacity Management Checklist (Appendix B)

5.11. Evidence of the reviewed checklist(s) must be retrained.

5.12. The ICT Manager must ensure that the configuration of server equipment outsourced, co-located, or hosted by external/third-party service providers is defined in the contract with the service provider. At a minimum the definition must document:

- Host contact information and location of server equipment;
- Server hardware and operating system/version;
- Server equipment purpose/function and applications;
- Configuration change management processes;
- Back-up requirements;
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO); and
- Escalation procedures.

5.13. IT reserves the right to isolate or otherwise disable without notice any server equipment that has been compromised by an attacker or, otherwise places the municipality's systems, data, users, and clients at risk as stipulated municipality's in the ICT Security Policy.

5.14. The ICT Manager and Senior IT Techinians as delegated by the ICT Manager must ensure that servers are named in accordance with the server and device naming conventions used by the municipality, to ensure consistency.

6. Monitor IT Infrastructure

6.1. Logging of infrastructure events must be maintained. All personnel must show due care in protection, handling, and storage of all monitored data and logs. The ICT Manager must ensure that logs record the following information on all business critical resources if the business requirements determine them to be relevant.

- User IDs;
- Dates/times and key events; and
- Workstation identification and location.

6.2. The ICT Manager must ensure that monitoring for the use of privileged operations occurs during the following instances:

- Systems are started or stopped;
- Input or output devices are attached or detached; and
- Changes and attempts to change security setting and controls.

6.3. The ICT Manager must ensure that monitoring for system alerts and failures capture the following details:

- Alerts or messages from consoles;
- Exceptions in system logs;
- Alarms generated by network management devices or access control systems; and
- Logs required by the business.

6.4. The ICT Manager must ensure that monitoring for system access captures the following details:

- The ID of the user;
- The date / time of key events;
- The type of event;
- The files accessed and their type; and
- The programs or utilities used during access.

6.5. Rules that identify and record threshold breaches and event conditions must be defined and implemented. A balance must be found between logging minor events and significant events so event logs are not logging unnecessary information, thus impacting data storage capacity.

6.6. The following IT infrastructure capacity planning elements must be monitored:

- Server CPU utilisation - check if CPUs are running at full capacity or are they being under-utilised. By monitoring server CPU utilisation, you can monitor server performance and restart a process or application to improve response time for the application;
- Server Disk utilisation - Monitor the hard disk space utilised by the system and ensure critical processes on the server have sufficient system resources;
- Server Process utilisation - Monitor memory and CPU utilisation of processes. This helps identify system processes or server applications using high Server Resources;
- Network Availability – to identify data bottlenecks or specific devices on the network using more resources than expected;
- Network traffic and Bandwidth usage - Monitor Network Interface traffic on the server and understand how much network load is being handled; and
- Network devices (routers, switches etc) – Ensuring that network devices are functioning as required.

6.7. Event logs and key indicators for critical systems and applications must be monitored and signed-off by an official independent of the process using the templates; Daily Operations Task Checklist document (Appendix A) and Monthly ICT Performance and Capacity Management (Appendix B)

6.8. Incidents must be logged, as per the Helpdesk and Incident Management Policy, in a timely manner when monitoring activities result in the identification of deviations and/or violations.

6.9. Infrastructure monitoring reporting must be provided by service providers on a monthly basis to provide feedback. Areas that must be covered are:

- Call logging statistics and statuses;
- Reports on the LAN and WAN infrastructure (Routers, switches, WAN interfaces etc.);
- Backup logs and reports; and
- Incidents that occurred in any of the above areas.

7. Appendices

A. Daily Operations Task Checklist document

B. Monthly ICT Performance and Capacity Management

Appendix A

Daily Operation Tasks Checklist:_____ Date:_____	
Network	
Network Availability	
Exceptions in system firewall logs	
Network traffic and Bandwidth usage	
Review alerts from antivirus console	
Virus Definitions updated for Antivirus	
Server Monitoring	
CPU utilisation	
Disk Space	
Process utilisation	
Backup	
Backup for all critical application/data was successful	
Independent review of Event Logs for Systems and Applications	
Review Application Logs for Error Events	
Review All System / Application Event Logs for Warnings	
Record Errors and/or Warnings	
Respond to Failures / Problems	
Systems are started or stopped	
Input or output devices attached or detached	

Daily Operation Tasks Checklist:_____ Date:_____

Independent review of Security Logs	
Successful and unsuccessful system access attempts	
System configuration changes	
Privileged access use	
System and application utilities use	
Changes and attempts to change security setting and controls	

Sign-offs

Performed by:	
Designation:	
Sign:	
Date:	
ICT Manager:	
Where there any Security Incidents? (Yes/No). **If yes, provide details and Incident No. and resolution**	
Sign:	
Date:	

Appendix B

Monthly Performance and Capacity Management Checklist: _____ Date: _____

Server	CPU Performance	Hard Drive Free Space	Memory Capacity	Comments

Monthly Performance and Capacity Management Checklist: _____ Date: _____				
Server	**CPU Performance**	**Hard Drive Free Space**	**Memory Capacity**	**Comments**
Checked by:				
Designation:				
Sign:				
Month:				

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS POLICY

Table of Contents

7. INTRODUCTION

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Physical and environmental safeguards are often overlooked but are very important in protecting information. Buildings and rooms that house information and information technology systems must be afforded appropriate protection to avoid damage or unauthorised access to information and systems. In addition, the equipment housing this information (e.g. filing cabinets, data wiring, laptop computers, portable disk drives, etc.) must be physically protected. Equipment theft is of primary concern, but other issues should be considered, such as damage or loss caused by fire, flood, and sensitivity to temperature extremes.

8. OBJECTIVES

The goal of the Physical Security and Environmental Controls Policy is to ensure the prevention of unauthorised physical access, loss, damage or interference to AbaQulusi Municipality's premises and infrastructure or interruptions to its critical operations, using physical and environmental controls appropriate to the identified risks and the value of the assets protected. As such, the main objectives of this policy are to:

a. To prevent unauthorised access, damage and interference to municipal premises and information.
b. To prevent loss, damage or compromising of assets and interruption to municipal activities.
c. To prevent compromising or theft of information and information processing facilities.

9. SCOPE

This policy applies to all individuals within the AbaQulusi Municipality that are responsible for the installation and support of information resources, individuals charged with information resources security and data owners.

10. Policy and Procedures

4.1. PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

4.1.1. This policy applies to full and part time employees, contractors, vendors, consultants and externally employed people who require computer room access.

4.1.2. It is essential that critical information is housed in secure areas, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference, commensurate with the identified risks.

4.1.3. The following guidelines and controls will be considered and implemented where appropriate:

4.1.3.1. Security perimeters are to be clearly defined.

4.1.3.2. A manned reception area or other means to control physical access to the site or building should be in place.

4.1.3.3. The computer room shall be kept locked by the ICT Manager and the keys shall be kept as follows:

4.1.3.3.1.1. One set with the ICT Manager;

4.1.3.3.1.2. One set with the Information Technology Officer;

4.1.3.3.1.3. Two sets with the two (2) Senior IT Technicians;

4.1.3.3.1.4. One set with the Delegated Server related IT Technician.

4.1.3.4. Access to sites and buildings should be restricted to authorised personnel only.

4.1.3.5. Visitor's time of entry and exit to the computer room should be recorded.

4.2.SECURING OFFICES, ROOMS AND FACILITIES

4.2.1. A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of secure areas must take into account the possibility of damage from fire, flood, explosion, civil unrest and other forms of natural or man-made disasters. Consideration must also be given to any security threats posed by neighbouring premises, i.e. leakage of water from other areas.

4.2.2. Disaster recovery equipment and backup media must be sited at a safe distance away to avoid damage from a disaster at the main site.

4.3.EQUIPMENT SITING AND PROTECTION

4.3.1. Equipment must be sited or protected to reduce risks from environmental threats and hazards, as well as opportunities for unauthorised access.

4.3.2. Protection of equipment (including that used off-site such as notebook computers for example) is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage.

4.3.3. As such, the following controls must be considered:

4.3.3.1. Equipment must be sited to minimise unnecessary access into work areas.
4.3.3.2. Controls must be adopted to minimise the risk of potential threats including:
4.3.3.3. Theft
4.3.3.4. Fire
4.3.3.5. Explosives
4.3.3.6. Smoke
4.3.3.7. Water (or supply failure)
4.3.3.8. Dust
4.3.3.9. Vibration
4.3.3.10. Electrical supply interference (or supply failure)

4.3.4. Over and above provisions that may be contained in the conditions of service, the use of alcohol (or other forms of substance abuse in secure areas or in the proximity of information processing facilities is expressly prohibited.

4.3.5. Consumption of food or beverages in secure areas or in the proximity of information processing facilities must not be allowed.

4.3.6. Other items prohibited within the Computer Room:

4.3.6.1. Combustible materials such as paper and cardboard (except reference manuals as needed)
4.3.6.2. Explosives and weapons
4.3.6.3. Hazardous materials
4.3.6.4. Alcohol, illegal drugs and other intoxicants
4.3.6.5. Electro-magnetic devices that could cause interference with computer and telecommunications equipment
4.3.6.6. Radioactive materials
4.3.6.7. Photographic or recording equipment (other than backup media)

4.4.POWER SUPPLIES

4.4.1. Key equipment must be protected from power failures and other anomalies. A suitable electrical supply conforming to the equipment manufacturer's specifications must be assured. To do so may require one or more of the following:

4.4.1.1. Multiple feeds to avoid a single point of failure in the power supply,
4.4.1.2. Uninterruptible Power Supply (UPS).

4.4.2. A UPS to support orderly shutdown or continuous running is necessary for equipment supporting business-critical operations. Contingency plans must cover the action to be taken in the event of failure of the UPS. UPS equipment must be regularly checked to ensure adequate capacity and tested in accordance with the manufacturer's recommendations.

4.4.3. Lightning protection may be necessary in certain buildings and lightning protection filters should be fitted to all external communications lines.

4.5. CABLING SECURITY

4.5.1. Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

4.5.2. As such, the following controls should be considered:

4.5.2.1. Power and telecommunications lines into the Computer Room should be underground, where possible, or subject to adequate alternative protection.

4.5.2.2. Network cabling should be protected from unauthorised interception, or damage, through (for example) the use of conduit or by avoiding routes through public areas.

4.5.2.3. Power cables should be segregated from communications cables or shielded to prevent electromagnetic interference.

4.5.2.4. Cables should be clearly marked and neatly arranged in cable racks.

4.6. AIR CONDITIONING

4.6.1 Air conditioning must be provided throughout the computer room. The temperature in the Computer Room must not go below 10°C or above 28°C. Use good quality racks to protect equipment, maximise efficient use of space and support the efficient distribution of chilled air.

4.6.2 Humidity in the computer room must be between 40% and 60% rH. Should the room be too dry, this will result in the build-up of static electricity on the systems. If it is too humid, corrosion will start slowly damaging the equipment resulting in permanent equipment failures.

4.7. DUST PREVENTION

4.7.1. The Computer Room must remain dust free at all times, therefore packing or unpacking of equipment should take place outside the room. Items can be unpacked in another room prior to introduction into the computer room with the help of staff.

4.7.2. Cardboard and other items that can generate dust and are easily combustible must remain outside the Computer Room. A waste bin should be available within the Computer Room for all other items of waste.

4.7.3. The Computer Room should be cleaned on a weekly basis.

4.8. FIRE DETECTION AND FIRE EXTINGUISHERS

4.8.1. The Computer Room must be fitted with a fire detection system that would notify the alarm company. The alarm company will then notify the ICT Manager should there be a fire within the computer room.

4.8.2. Hand held fire extinguishers that are safe for computing systems should be located in and outside of the computer room.

4.9.EQUIPMENT MAINTENANCE

4.9.1. Equipment must at all times be correctly maintained to ensure continued availability and integrity, compliance with warranty provisions and protection of the municipality's investment.

4.9.2. As such, the following controls must be considered:

4.9.2.1. Equipment must be maintained in accordance with the manufacturer's recommendations and according to the manufacturer's recommended service intervals and specifications.

4.9.2.2. Only authorised maintenance personnel may carry out repairs and service equipment.

4.9.2.3. Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.

4.9.2.4. Appropriate procedures and controls must be applied when equipment leaves municipal premises for maintenance (in particular, the confidentiality and security of data that may be stored in the

equipment must be considered). Also, stringent recording procedures must be applied in order to track the whereabouts of the equipment.

4.10. RAISED FLOORING

4.10.1. All servers and electrical equipment/ cabling must be raised above the ground to prevent damage during a flood or burst water pipes that may affect the computer room.

4.10.2. In addition, raised flooring will assist with the protection of data cables as these will be located under the raised floor.

4.11. SECURE DISPOSAL OR RE-USE OF EQUIPMENT

4.11.1. Information security can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information should be physically destroyed or securely overwritten, rather than simply using the standard 'delete' function which effectively resets the file size to zero without destroying the data.

4.11.2. In cases of extreme sensitivity, it may be necessary to overwrite the disk up to seven times or use a degausser or perform a low-level format to ensure that the data is irrecoverable.

4.11.3. Final disposal of information processing equipment, in common with all municipal movable assets, is subject to the provisions of any other applicable policies and/or procedures.

4.12. GENERAL CONTROLS

4.12.1. Information and information processing facilities must be protected from disclosure to or modification by unauthorised persons, or theft. Effective controls must be implemented to minimise the risk of loss or damage.

4.13. CLEAR DESK AND CLEAR SCREEN PRACTICES

4.13.1. It is recommended that “clear desk” and “clear screen” practices become the norm at all municipal premises, so that removable media and information contained in paper reports are not visible or accessible to unauthorised persons. Information storage media left on desks is also more likely to be damaged in the event of a disaster and to reduce the risk of unauthorised access to facilities.

4.13.2. The following controls should be considered and implemented where appropriate:

4.13.2.1. Paper documents and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside of working hours.

4.13.2.2. Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.

4.13.2.3. Personal computers and computer terminals must not be left logged on when unattended and should be protected by key locks, screensavers with passwords or other controls when unattended.

4.13.2.4. Personal computers and computer terminals must not be left switched on overnight. The normal switch on and “boot up” process also carries out certain housekeeping functions that are necessary for optimum functioning.

4.13.2.5. Sensitive or classified information, when printed, should be cleared from printers immediately. Business units who regularly need to print such documents should consider a personal printer rather than using shared facilities, where appropriate.

4.14. REMOVAL OF PROPERTY

4.14.1. Equipment, information or software must not be taken off-site without proper authorisation.

4.14.2. Where necessary and appropriate, equipment should be logged out and logged back in when returned.

11. ENFORCEMENT

Non-compliance, violation and disregard of this policy by any AbaQulusi Municipality employee, consultants and temporary staff shall result in disciplinary action and sanctions against the individual concerned and such sanctions may lead to termination of the individual's employment contract, depending on the circumstance and the gravity of the transgression. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and/or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the individual and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the individual.

APPENDIX A: REMOVAL OF IT EQUIPMENT

Equipment Description	Serial Number	Name and Surname of User	Signature of User	Date	Name and Surname of Approver	Signature of Approver	Date

USER ACCOUNT MANAGEMENT POLICY

TABLE OF CONTENTS

1. Introduction

The main goal of Information Security is to protect the municipality's information resources from risks that affect the confidentiality, integrity and availability of the information. One of the main protection mechanisms implemented in the municipality to achieve this goal is effective Access Control. Access Control is generally seen as the first step in providing Information Security and therefore merits the proper implementation and management thereof in the municipality. Access Control is important as it allows a user access to the municipality's information resources.

Logical access to the municipality's information assets needs to be managed in a controlled manner and logical access permissions granted on the basis of business requirements. Lack of adequate logical access controls could lead to unauthorised access to information and information assets.

2. Objective

This document defines the procedures for effective management of logical access to AbaQulusiMunicipality's information resources.
The purpose of this policy is to ensure the effective and efficient management of access to the municipality's information resources and systems and includes:

- Granting access after relevant management authorisation and an official request has been received.
- Removing access upon role change, service termination or contract expiry.
- Resetting of access on positive identification of the owner of the user ID as the requestor.
- Updating access as required after an official authorised request has been received.
- Regularly reviewing the granted access privileges of users to determine whether they are still valid and necessary.

3. Scope

This policy applies to all computer and communication systems owned or operated by AbaQulusiMunicipality and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

4. Authority & responsibility

This policy affects all employees of AbaQulusi Municipality and its subsidiaries and all contractors, consultants, temporary employees and business partners. Employees who

deliberately violate this policy will be subject disciplinary action up to and including termination.

5. Definitions and acronyms

IEEE – The Institute of Electrical and Electronics Engineers is a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence. It is one of the leading standards-making organisations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards Association (IEEE-SA). IEEE standards affect a wide range of industries. One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking standard.

Firewall– A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorised access while permitting legitimate communications to pass.

Remote Access is access to the Local Area Network (LAN) from any location outside the firewall by any method, including but not limited to Virtual Private Network (VPN), dial-in modem, frame-relay, SSH, cable-modem and any other method of accessing the LAN from outside the firewall.Remote access can refer to remote desktop, remote terminal (like Telnet) or any type of remote application / device (including remote browser).

Operating System – An operating system (OS) is a set of programs that manage computer hardware resources and provide common services for application software. The operating system is a vital component of the system software in a computer system.

LAN – A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.

VPN – A virtual private network (VPN) is a secure network that uses primarily public telecommunication infrastructures, such as the Internet, to provide remote offices or travelling user's access to a central organisational network. VPNs typically require remote users of the network to be authenticated, and often secure data with firewall and encryption technologies to prevent disclosure of private information to unauthorised parties.

PDA – A personal digital assistant, also known as a personal data assistant, is a mobile device that functions as a personal information manager. Current PDAs often have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, but some newer models also have audio capabilities, enabling them to be used as mobile phones or portable mediaplayers.

Many PDAs can access the Internet, Intranets or Extranets via Wi-Fi or Wireless Wide Area Networks. Many PDAs employ touch-screen.

Wi-Fiis a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as "WLAN".

SSH – Secure Shell is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs). The protocol specification distinguishes two major versions referred to as SSH-1 and SSH-2.

SCP –Secure Copy is a means of securely transferring files between computers. It is based on the Secure Shell (SSH) protocol. The term SCP can refer to the SCP protocol or the SCP program.

SFTP – The SFTP command is a command-line interface client program implementing the client-side of the SSH File Transfer Protocol as implemented by the SFTP-server command by the OpenSSH project, which runs inside the encrypted SSH connection. It provides an interactive interface similar to traditional FTP clients.

Telnet – a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection.

6. Policy

6.1 Authorised Users

6.1.1. Only authorised users are granted access to information systems and users are limited to specific defined, documented and approved applications and levels of access rights.

6.1.2. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

6.2 Authentication

6.2.1. Any User (remote or internal), accessing AbaQulusi Municipality networks and systems must be authenticated.

6.2.2. Entity authentication includes but is not limited to:

6.2.3.1. Automatic logoff

6.2.3.2. A unique user identifier

6.2.3.3. And at least one of the following:

6.2.3.3.1. Biometric identification

6.2.3.3.2. Password

6.3 Workstation Access Control

6.3.1. All workstations used for AbaQulusi Municipality business activity, no matter where they are located, must use an access control system approved by AbaQulusi Municipality. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a logon password to access the computer.

6.3.2. When a user leaves a workstation, the user is expected to properly log out of all applications and networks.

6.3.3. Users will be held responsible for all actions taken under their sign-on. This minimises the opportunity for unauthorised users to assume the privileges of the intended user during the authorised user's absence.

6.4Disclosure Notice

6.4.1. A notice warning that those should only access the system with proper authority will be displayed initially before signing on to the system.

6.4.2. The warning message will make clear that the system is a private network or application and unauthorised users should disconnect or log off immediately.

6.5System Access Controls

6.5.1. Access controls will be applied to all computer-resident information based on its' Data Classification (refer to the ICT Security Policy) to ensure that it is not improperly disclosed, modified, deleted or rendered unavailable.

6.6Access Approval

6.6.1. System access or modification to access will not be granted to any user without appropriate approval first.

6.6.2. Management is to immediately notify the ICT Manager and report all significant changes in end-user duties or employment status. The ICT Manager should also be informed as to how access rights on systems should be updated due to role changes.

6.6.3. User access is to be immediately revoked or disabled if the individual's employment has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job role.

6.7 Limiting User Access

6.7.1. AbaQulusi Municipality approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorised.

6.8 Privileged / Super User Access

6.8.1. For security reasons AbaQulusi Municipality must limit the number of super users in the municipality only to individuals who have a justifiable business use for such access.

6.8.2. An approval process for granting and requesting super user will be followed.

6.9 Resetting a Password

6.9.1. All password reset requests must be done by completing a User Access Form and handing it to the Helpdesk which needs to follow the stipulated levels of approval as per the User Access Form.

6.9.2. A change of password is forced on the first logon with the reset password.

6.10 Periodic Review of User Profiles and Access Rights

6.10.1. A review of all User Accounts must be performed on an annual basis by the appropriate business unit Managers and the ICT Manager.

6.10.2. This is done by verifying user permissions and group memberships against the master user register.

6.10.3. The review must also include the identification of inactive accounts. An account is deemed 'inactive' where it has not been used within 60 days. Inactive accounts must be removed from the system immediately after the 60 days has elapsed. This would only apply for User Accounts, not System Accounts.

6.10.4. System accounts will be setup to not allow logon.

6.11 Access Privilege

6.11.1. Users will be granted access to information on a least privilege basis. That is, users will only receive access to the minimum applications and privileges required for performing their relevant jobs.

6.12 Compliance

6.12.1. Users who access AbaQulusi Municipality's information systems must sign a compliance statement prior to issuance of a user ID. Refer to the AbaQulusi Municipality's ICT Security Policy and Procedures for further details.

6.12.2. A signature on this compliance statement indicates the user understands and agrees to abide by AbaQulusi Municipality's policies and procedures related to computers and information systems.

6.12.3. Annual confirmations will be required of all system users.

6.13 Audit Trails and Logging

6.13.1. Logging and auditing trails must be reviewed periodically by the ICT Manager.

6.14 Access for Non-employees

6.14.1. Individuals who are not employees, contractors, consultants or business partners must not be granted a User ID or otherwise be given privileges to use AbaQulusi Municipality's computers or information systems unless the written approval of the relevant Department Heads has first been obtained and then sent to and approved by the ICT Manager accordingly.

6.15 Unauthorised Access

6.15.1. Employees are prohibited from gaining unauthorised access to any other information systems or in any way damaging, altering or disrupting the operations of these systems.

6.15.2. System privileges allowing the modification of 'production data' must be restricted to 'production' applications only.

6.16 Remote Access

6.16.1. Any employee using any computing device remotely must ensure that such a device is updated with the most recent security patches for their Operating System. Please refer to the AbaQulusi Municipality's Patch Management Policy for details regarding patch management.

6.16.2. All machines on the AbaQulusi Municipality's LAN as well as any remote computing device must run the most up-to-date versions of antivirus software with regularly updated virus definitions, i.e. at a minimum, once

a day. However, whenever deemed necessary by the ICT Department, these updates may be required to run more frequently due to business requirements. Please refer to the AbaQulusi Municipality's Patch Management Policy for details regarding antivirus updates.

6.16.3. Any authorised user using a remote computing device outside the firewall must use the VPN to send and receive AbaQulusi Municipality's email or to access the Internet and Intranet accordingly. No AbaQulusi Municipality's email may be sent using third-party email services (including, but not limited to, Gmail, Hotmail, Webmail, etc.). Please refer to the AbaQulusi Municipality's End User Security Policy for details regarding remote access and VPN.

6.16.4. Any authorised user accessing any computer or device on the LAN for remote management or administration must use SSH and/or VPN. For remote file transfer, employees must use VPN. Under no circumstances shall Telnet, FTP or any other unencrypted access methods be used.

6.16.5. All employees using any computing device to remotely access and connect to AbaQulusi Municipality's LAN shall not do so while still connected to any other network.

6.16.6. All employees requiring remote access to AbaQulusi Municipality's LAN need to complete and submit a Change Request Form to the ICT Manager for relevant approval first. Please refer to the AbaQulusi Municipality's IT Security Procedure for details regarding the provision of remote access to the AbaQulusi Municipality's network.

6.17 Registration of new users

6.17.1. HR must notify IT to create a new user account. The IT User Access form must be completed and approved by the relevant authority. Relevant access will be granted by the ICT Manager upon receipt of the approved IT User Access form.

6.18 Termination procedures

6.18.1. HR must notify IT prior to the termination of an employee's employment to ensure that access is revoked on the employees last working day.

6.18.2. The employee's user account will be removed and the master user register will be updated to reflect the user account has been removed.

7. Enforcement

7.1. Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanctions against the employee concerned and such sanctions may lead to termination of the employee's employment contract, depending on the circumstance and the gravity of the transgression.

7.2. In the event of AbaQulusi Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, AbaQulusi Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user and this shall be in addition to the disciplinary action that AbaQulusi Municipality would have taken against the employee.

8. Cross-reference to other policies/procedures

8.1. User Access Management Procedure

9. Reference Material Used In Developing This Policy

9.1. IEEE Wireless Networking Standards

INFORMATION COMMUNICATION AND TECHNOLOGY
USER ACCOUNT MANAGEMENT PROCEDURES

Table of Contents

1. Purpose

The purpose of the AbaQulusi Municipality User Account Management Procedure is to maintain an adequate level of security to protect AbaQulusi Municipality data and information systems from unauthorised access. This procedure defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of AbaQulusi Municipality information systems.

2. Scope

This procedure document applies to all computer and communication systems owned or operated by AbaQulusi Municipality and its subsidiaries. Similarly, these procedures apply to all platforms (operating systems) and all application systems.

3. User Access Procedures

3.1. New Users or Modified Access

3.1.1. A user will log a call with the IT Helpdesk requesting access or modification of access to the network or to an application.

3.1.2. The IT Helpdesk will log the call in CCM, which is the helpdesk system used by AbaQulusi Municipality.

3.1.3. The User Access Form (see Appendix A) will then be sent to the users' manager or be provided directly to the user.

3.1.4. The user must then complete the User Access Form, sign it and submit the form to his / her Line Manager for approval.

3.1.5. The users' Line Manager will review the access applied for by the user and determines if the access requested is in accordance with the system function required for the staff member to perform his/her duties.

3.1.6. The Line Manager will then sign and date the form as acknowledgement of approval.

3.1.7. If the user requires access or modification of his/her access to the financial system, the user must select what type of access is required and submit the form to the CFO.

3.1.8. The CFO must review the access permissions selected by the user and provide approval of said accesses before access to the financial system will be granted/modified by the ICT Manager.

3.1.9. The completed and approved User Access Form must then be submitted to the ICT Manager.

3.1.10. The ICT Manager will review the User Access Form to ensure that the information is complete and valid authorisation has been provided in accordance with the system security baseline for each application to ensure that the access requested does not provide excessive system access or conflicting roles.

3.1.11. The ICT Manager must also establish whether the employee is entitled to the access / requires modified access (i.e. relevant enquiries must be made through Human Resources to validate employment accordingly).

3.1.12. The ICT Manager must sign and date the form as acknowledgement of approval.

3.1.13. The ICT Manager or Information Technology Officer will then grant access as per the User Access Form and will use the standard naming convention as stipulated in 3.1.14.

3.1.14. The following user account naming convention must be used so that user ID's are unique to enable easy identification of users allocated access and also prevent the possibility of duplicate system account IDs:

Ref No	Application	Naming Convention
1	All Systems	Initial/s with full surname (e.g. JSmith)

3.1.15. The ICT Manager or Information Technology Officer will then notify the user that access has been granted/modified via email or telephone.

3.1.16. The User Access Form must be filed and retained for audit purposes.

3.1.17. Where the system functionality allows it, the user must change their password at their first subsequent login.

Note: If an individual is acting in a position that requires elevated access then proof of said acting position is required.

3.2. Termination of User Access

3.2.1. The Human Resources (HR) department must send a monthly Terminations Listing Report to the ICT Manager to identify employees whose access must be deleted at month end.

3.2.2. Upon receiving the termination notifications, the ICT Manager or Information Technology Officer must then delete all terminated employees access on the relevant systems immediately.

3.2.3. The ICT Manager or Information Technology Officer will then notify the relevant Line Managers via email that the terminated employees have had their access removed on the relevant system(s) accordingly.

3.3. Password Resets

3.3.1. If a user requires their password to be reset, the user will log a call with the IT Helpdesk.

3.3.2. The IT Helpdesk will capture the call details in CCM.

3.3.3. The User Access Form (see Appendix A) will then be sent to the user by the it Helpdesk.

3.3.4. The user must complete their details under 'User information' in the User Access Request Form and by ticking the box 'Reset Password'.

3.3.5. The completed User Access Request Form must be returned to the it Helpdesk.

3.3.6. The it Helpdesk will then handover the User Access Request Form to either the ICT Manager or the Information Technology Officer.

3.3.7. The ICT Manager or the Information Technology Officer will reset the password upon verification of the user's identity.

3.3.8. The change password at next logon policy must be ticked and enforced by the ICT Manager or the Information Technology Officer, so that the user will be required to change their password when their password is reset.

4. Periodic Review of User Profiles and Access Rights

4.1. A review of all user accounts must be performed on an annual basis by the organisation (Heads of Department).

4.2. This is done by verifying if the user's permissions and access rights are commensurate with their current role and responsibilities.

4.3. The ICT Manager will provide the access rights of staff to the Heads of Department for review.

4.4. The Heads of departments must flag inappropriate access and sign-off the access lists. This should be retained by IT as evidence.

4.5. Where inappropriate access is identified, the access should be removed or amended as appropriate by the IT Department.

4.6. The review must also ensure that user IDs are linked to specific individuals by specifying the name and surname of the user concerned against each user ID.

4.7. The review must also include the identification of inactive/ dormant user accounts. An account is deemed 'inactive' where it has not been used within 60 days. Inactive accounts must be removed from the system. This would only apply for User Accounts and not System Accounts.

4.8. Appropriate evidence of review must be retained and filed.

5. Enforcement

If any AbaQulusi Municipality staff member is found to have breached this procedure document, they may be subject to disciplinary action, up to and including termination of employment. Any violation of this procedure document by a temporary worker, contractor or supplier may also result in the termination of their contract or assignment accordingly.

6. Appendices

A. User Access Request Form

Appendix A: User Access Request Form

Help Desk No.	

New User		Existing User		Re-Instate User		Delete User		Un/Lock User		Reset Password	

User Information:			
First Name		**Last Name**	
Employee Number		**Department**	
E-mail address		**Telephone Number**	
Line Manager		**Other**	

Access Requested To:			
☐ Internet	☐ Email	☐ Contour	☐ ESS
☐ MunSoft	☐ Arc GIS	☐ Caseware	☐ Network
☐ MunAdmin EDMS	☐ Payday	☐ TCS	☐ Other
If other, specify _____			

Menu Access:			
☐ Consumer Debtors	☐ Creditors	☐ Sundry Debtors	☐ Cashbook
☐ Cashier	Stores ☐ ACB	☐ Fixed Assets	☐
☐ General Ledger	☐ Salaries	☐ Costing	☐ta Transfers

Financial System Access:			
☐ Manager Enquiries Only	☐ Cashbook Users	☐ Fixed Asset User	☐ Creditors Enquiries
☐ Management Authorisation	☐ Cashbook Enquiries	☐ GL User	☐ Stores User
☐ Consumers User	☐ Debtors Users	☐ GL Enquiries	☐ Stores Enquiries
☐ Consumers Enquiries	☐ Debtors Enquiries	☐ Creditors User	☐ Procurement User
☐ Procurement Enquiries	☐ Costing User	☐ Costing Enquiries	☐ Other

If other, specify _____

Authorisation Information:					
Completed by		Signature		Date	
Authorised by Line Manager		Signature		Date	
Authorised by CFO (Financial System only)		Signature		Date	
Authorised by ICT Manager		Signature		Date	
Access Granted by		Signature		Date	

Additional Comments

NEW ADDITIONAL DOCUMENTS

MOBILE DEVICE MANAGEMENT AND ACCEPTABLE USE POLICY

MOBILE DEVICE MANAGEMENT AND ACCEPTABLE USE POLICY

PREAMBLE

AbaQulusi Local Municipality continuously endeavours to achieve the best policies and procedures when managing the administration and operations of the assets of the Municipality.

In order to enable and enhance excellent communication and productivity of all Municipality's business units, it is critical to make use of the latest communication technology techniques . Based on this, technology mobile devices (e.g. smart phones, tablets, mobile routers, laptops, etc.) are then encouraged and allocated to specific senior managers, managers, assistant managers or specialist employees as tools of trade for sound business reasons.

LEGISLATIVE FRAMEWORK

Local Government: Municipal Structures Act 117 of 1998;

Local Government: Municipal Systems Act No 32 of 2000;

Remuneration of Public Office –bearers Act, 1998(No. 20 of 1998)

Municipal Finance Management Act 56 of 2003;

State Information Technology Act, 1998 (88 of 1998);

Protection of Personal Information Act, No4 of 2013;

Electronic Communications Security Act, 2002(Act 68 of 2002);

ICASA (Independent Communications Authority of South Africa);

AbaQulusi Municipality Information Communication Technology Policy;

AbaQulusi Municipality Supply Chain Policy;

AbaQulusi Municipality Asset Management Policy;
AbaQulusi Asset Management Policy;

DEFINITIONS

Municipality means the AbaQulusi Local Municipality

Councillor means a person who has been elected by the voters of the public (in terms of the Municipal Structures Act 117 of 1998) to look after the needs and the entire service delivery to the certain community Ward.

Municipal Manager means a person who has been been appointed by the Municipality in terms of section 54 of the Municipal Systems Act and who is the Head of the Administration and also the Accounting Officer for the Municipality.

Director or Head Of Department means a person who has been appointed by the Municipality in terms of section 56 of the Municipal Systems Act and who is the Head of a department within AbaQulusi Municipality.

Level 18-0 Means an employee appointed by the Municipality on a post level 18-0 at the Manager Level

Level 0-18 means an employee appointed by AbaQulusi Municipality on a post level 14 at the Assistant Manager Level

Other Personnel means any other personnel appointed by AbaQulusi Municipality on post levels 1 to 16

1. Application of the Policy

This Policy shall apply to :

1.1. The Honourable Councillors
1.2. The Municipal Manager
1.3. Section 56 Managers
1.4. Level 18-0 Employees,
1.5. Post level 14
1.6. To any other official (e.g. Technicians , Specialists, etc. who had received approval from the Municipal Manager to be granted a mobile device such as a Tablet and or a Smartphone thereof.

2. The Mobile Device Provision

The Functional term of the Mobile Device (Tablet)

In terms of the AbaQulusi Municipality Asset Policy jointly with the ICT Policy, it is indicated that the functional term for the mobile device (e.g. Tablet) shall be a period

of 5 years, hence after the first two years of payment, the tablet fee will fall out or discontinue then the Municipality will only be beneficially running a month to month minimum subscription fee plus insurance until the end of the above mentioned functional term

As stipulated in the introduction above that AbaQulusi Municipality is committed to enhance effective ways and means of modern communication through provision or allocation of mobile tools of trade such as Tablets to the honourable councillors, senior managers, managers, specific specialist employees as approved for by the Municipal Manager who is an Accounting officer of the Municipality.

Furthermore all mobile device users listed above shall receive Tablets as the chosen mobile devices or tools of trade that are afforded or paid for by the Municipality in full through monthly instalments.

Therefore the structure of the Tablets total payment per device is as follows:

a) The monthly device or tablet amount
b) The monthly data subscription fee
c) The Insurance monthly premium for (Loss, damage and theft)

In addition ,Senior management and all other employees mentioned above (also as approved by the Accounting Officer)shall pay the data subscription fee until the end of the functional term through their cell phone allowances .

Hence these mobile devices shall be written on an asset register which means that they should be tagged with asset numbers and each allocated mobile device shall be upgraded after each functional term, as a result after new mobile devices have been received, the old ones shall be returned to ICT and Assets sections for verification and disposal.

Any mobile device purchased using AbaQulusi Account on behalf of any official who has a cell phone allowance, financial expenditure section will deduct the entire amount back to the municipality account from the that particular official , hence the device shall remain the Asset of abaQulusi Municipality until the end of the contract, therefore should the Official leave the Municipality or pass on before the end of the contract then the Mobile Device should be returned back to AbaQulusi Municipality ICT Department which means the Municipality has a full right to reallocate such contracted device.

In addition a Councilor shall be provided tools of trade by the Municipal Council to enable such councilor to discharge his or her duties in the most efficient and effective manner , therefore mobile devices(i.e. tablets) shall be freely allocated to the Councilors and therefore the Municipality shall bear the costs in total as per the illustrated total payment structure above as the electronic agendas and any other necessary documents are uploaded in these tablets as an official tool of trade, as a result the tablet shall remain an asset of AbaQulusi Municipality during the 5 year serving term of an honorable councilor , hence it had been agreed upon by the Municipal Council that after finishing a five year term each councilor should preserve the tablet as it would be out of warranty.

In the case where an honorable councilor have not finished his or her term of office (due to resignation, dismissal , death or any unforeseen reason which may cause a bi-election), the tablet must be returned to the Municipality and be handed over to the newly elected councilor.

.

3. The Mobile Device Security

It is primarily a responsibility of each and every mobile device user to install the antivirus on his or her own allocated device using Google play store or other relevant apps, furthermore should the user experience difficulty during the endeavour to install the above mentioned security feature, they must visit the ICT Office for assistance.

In addition, it is also the responsibility of each and every mobile device user to create password for his or her own allocated device for confidentiality purposes.

4. Data Usage

Mobile Device Data is a very crucial resource for mobile devices as it ensures connectivity to the internet. Furthermore the every mobile device user is provided with enough data bundles from a minimum 10GB through an affordable, cost effective monthly subscription fee which is paid by Council, therefore mobile device users are expected to consume these data bundles strictly for work purposes i.e. virtual meetings, video conferencing, work related research, work related internet surfing, etc. Hence sticking to the above mentioned data usage rule can protect these devices from unacceptable uses and it can also save time and money for the Municipality.

CURRENT ICT STEERING COMMITTEE TERMS OF REFERENCE

APPROVAL

This Information Communication Technology Policy was approved by the following:

_____ _____

Chairman of the ICT Steering Committee **Date**

_____ _____

Chairman of the Corporate Services Portfolio Committee **Date**

_____ _____

Chairman of the Executive Committee **Date**

_____ _____

Chairman of the Council **Date**

_____ _____

Acting Municipal Manager **Date**