




UMZIMKHULU LOCAL MUNICIPALITY



Name	ICT OPERATIONS POLICY
Status	ADOPTED
Approved By	Council
Date Approved	MAY 2020
Date Last Amended	December 2019
Date for Next Review	December 2020

APPROVAL

	Signature	Date
Senior IT Officer		08/06/20
Head of Corporate services		08/06/20
Municipal Manager		08/06/20

CONTENTS

1.	INTRODUCTION	5
2.	DEFINITIONS	5
3.	PRESCRIPTIVE/LEGAL FRAMEWORK.....	12
4.	POLICY OBJECTIVES:.....	13
5.	ICT SYSTEM ACQUISITIONS.....	13
5.1	POLICY PRINCIPLES.....	13
5.2	KEY PRINCIPLES AND GUIDELINES PERTAINING TO THE ACQUISITION OF ICT SYSTEMS/APPLICATIONS	13
6.	ICT HARDWARE & SOFTWARE.....	14
6.1	KEY PRINCIPLES AND GUIDELINES PERTAINING TO ICT HARDWARE OR SOFTWARE	15
6.2	KEY PRINCIPLES AND GUIDELINES PERTAINING TO COMPUTER SOFTWARE.....	16
7.	ICT SERVICE DESK (HELP DESK)	17
7.1	USE OF THE SERVICE DESK.....	17
7.2	REQUESTING ICT SERVICE OR ASSISTANCE.....	17
7.3	OPERATING HOURS OF THE ICT SERVICE DESK.....	18
8.	ICT FACILITIES, ENVIRONMENTAL STANDARDS & MAINTENANCE	18
8.1	ACCESS CONTROL.....	18
8.2	FIRE CONTROL	18
8.3	AIR CONDITIONING.....	19
8.4	UNINTERRUPTIBLE POWER SUPPLY (UPS)	19
8.5	CLEANLINESS	20
9.	DATA MIGRATION	20
10.	ICT CHANGE CONTROL MANAGEMENT	22
10.1	CHANGE MANAGEMENT RISK ASSESSMENT	23
10.2	CHANGE MANAGEMENT REVIEWS.....	23
10.3	CHANGE MANGEMENT TESTING.....	24
10.4	CHANGE MANAGEMENT PROCESSES.....	24
11.	WEBSITE MANAGEMENT	26
12.1	WEBSITE COMPLIANCE	26
12.2	WEBSITE MANAGEMENT AND GOVERNANCE	28
12.3	CONTENT MANAGEMENT GUIDELINES	29
12.	LICENCING MANAGEMENT	29
14.1	KEY PRINCIPLES AND GUIDELINES PERTAINING TO LICENCING MANAGEMENT	30
13.	BACKUPS AND RESTORES.....	30
15.1	KEY PRINCIPLES AND GUIDELINES PERTAINING TO DATA BACKUP & RESTORE	31
15.2	DATA BACKUP & RESTORE PROCEDURES	31
15.3	BACKUP CONTENT	32
15.4	BACKUP SCHEDULING.....	32
15.5	BACKUP TYPES	32
15.6	BACKUP TESTING AND RESTORE.....	32
15.7	DATA RETENTION.....	33
14.	MUNICIPAL STRUCTURE, ROLES, AND RESPONSIBILITIES	33
17.1	THE MUNICIPAL COUNCIL	33
17.2	THE MUNICIPAL MANAGER	33

17.3	THE ICT STEERING COMMITTEE, RISK, AND AUDIT COMMITTEE	34
17.4	RESPONSIBILITIES OF MANAGER: ICT	34
17.5	RESPONSIBILITIES OF FINANCIAL ADMINISTRATOR	36
17.6	RESPONSIBILITIES OF VENDORS AND CONTRACTORS	36
17.7	RESPONSIBILITIES OF USER DEPARTMENT	36
17.8	RESPONSIBILITIES OF COMPUTER USERS	37
17.9	RESPONSIBILITIES OF ICT STEERING, MANCO, RELEVANT PORTFOLIO AND EXECUTIVE COMMITTEES	37
17.10	RESPONSIBILITIES OF MANAGER: SUPPLY CHAIN MANAGEMENT	38
17.11	RESPONSIBILITIES OF PROJECT MANAGER	38
17.12	RESPONSIBILITIES OF MANAGER: INTERNAL AUDIT	38
17.13	RESPONSIBILITIES OF APPLICATION OWNERS	38
17.14	RESPONSIBILITIES OF SECTION MANAGERS/UNIT HEADS	39
17.15	RESPONSIBILITIES OF HEADS OF DEPARTMENTS	39
17.16	RESPONSIBILITIES OF MANAGER CORPORATE SERVICES	39
17.17	RESPONSIBILITIES OF NETWORK ADMINISTRATOR	39
15.	POLICY APPLICATION	40
16.	EXCEPTIONS TO THE PRINCIPLES OF THIS POLICY	40
17.	MONITORING AND EVALUATION	40
18.	COMMENCEMENT	41
19.	AMENDMENT AND/OR ABOLITION	41
20.	COMPLIANCE AND ENFORCEMENT	41
21.	POLICY REVIEW	41
22.	APPEAL PROCESS/ GRIEVANCE PROCEDURE	41
	Records of Approval	41

1. INTRODUCTION

Umzimkhulu Local Municipality expects that all ICT Systems, applications, and computer equipment be sourced through the Municipality's ICT Section, located in the Corporate Services Department or in the event of specific financial systems applications being required, through the Manager ICT Projects of the Treasury Department. As functional and technical support is provided by the ICT Section, compliance to this directive is mandatory.

This Policy further aims to provide the municipality with a framework and guidance in terms of steps and key factors to consider in planning, acquiring, implementing, and reviewing any ICT Systems' acquisitions.

It is the policy of Umzimkhulu Local Municipality to manage the lifecycle of all applications that support its business and technical objectives. These applications are subject to formal change control processes that provide a managed and orderly method by which changes are requested, approved, tested, communicated prior to implementation, and logged

One of the important data/information controls is regular backups of such and it makes sure that whatever hardware failures the municipality may experience, the municipality's data/information is safely stored for access or recovery when required.

2. DEFINITIONS

1	Acceptance Testing	Is a level of the software testing process where a system is tested for acceptability. The purpose of this test is to evaluate the system's compliance with the business requirements and assess whether it is acceptable for delivery.
2	Application	A system that provides a specific set of functions and/or services to end users in support of business objectives. The term is commonly associated with a specific software application such as a financial system.
3	Application Owner	The business owner of an application. This could be a manager of a department or section that uses the specific application in carrying out its business.
4	Application/System	A system that provides a specific set of functions and/or services to end users in support of business objectives. The term is commonly associated with a specific software application such as a financial system.
5	Asset	Anything that has value to the municipality
6	Change Control	Regulates the practices used to make modifications to the application or its environment to ensure appropriate authorization, testing, and successful production implementation of a change.

7	Change Management	Coordinates the application of changes into the environment to ensure there are no conflicting changes and communicating awareness of changes typically through a panel or review board process.
8	Change Management (Human Context)	An approach to shifting individuals, teams, and organisations from a current state to a desired future state. It is an organisational process aimed at helping change stake-holders to accept and embrace changes in their business environment.
9	Change Management (Technical Context)	Refers to a project management process where changes to a project are formally introduced and approved.
10	Commercial Off-The-Shelf Systems (COTS)	Computer systems that are widely available and are mass produced with general commercial application in mind. Examples are desktops, laptops, commercial accounting application, etc
11	Computer Hardware Refresh	The process of restoring the computer to its original form by re-installing the Operating system and, if necessary, other necessary software to improve its performance after some time of usage.
12	Computer Image	In the context of computer science, is the current copy of the hard disk. It saves the entire data from the disk, including the file structure, the operating system, installed applications and/software, and all files and folders from the disk, in a single file
13	Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. Control is also used as a synonym for safeguard or countermeasure
14	Data	Also known as values or variables, are qualitative or quantitative facts about things. Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.
15	Data Catalogue	A collection of models representing objects, such as business items and notifications, to be used as inputs and outputs in process modelling.
16	Data Centre	Is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls and various security devices. It is generally bigger than a server room.
17	Data Cleansing/Data Cleaning/Data Scrubbing	The process of detecting and correcting incomplete, incorrect, inaccurate, irrelevant, corrupt or inaccurate data in a system or database.

18	Data Cleanup	The act of deleting from a database those records for which the cleanup period has expired.
19	Data Density	The measure of missing values in the data and the number of total values ought to be known.
20	Data mapping	Refers to the process of identifying and linking data components from the legacy system to the new/destination system.
21	Data Migration	The transferring of data between storage types, formats, or computer systems. It is required when organizations or individuals change computer systems or upgrade to new systems.
22	Data Normalisation	In the context of this policy, this refers to the reduction and even elimination of data redundancy, i.e. making sure that there's no duplication of data on the new/destination system. This process ensures reduction of unwanted variations and inaccuracies in the data. It also ensures that data dependencies are kept intact prior to and after migration.
23	Data Profiling	Process used to identify data quality errors, uncover relationships that exist between different data elements, discover sensitive data that may need to be masked or hidden, and monitor data quality on an ongoing basis to support data governance.
24	Data Quality Analysis	Refers to the process of differentiating between good and bad data.
25	Designated Authority	The Manager: ICT as delegated by the Municipal Manager as the Information Security Officer or any other person delegated by Manager: ICT to act as Information Security Officer on his/her behalf.
26	Differential backups	Includes files that have been changed since the last Full (Clear Archive Bit) or Incremental backup. If the archive bit is on, the file is backed up, and archive bit is not turned off. The next time an incremental backup is done, this file is skipped (unless it is modified again).
27	Encryption	Is a technique that can be used to protect the confidentiality of information. It should be considered for the protection of sensitive or critical information
28	End User/Functional User/User	End Users are individuals who are widely characterized as the class of people that use a system without complete technical expertise required to understand the system fully. The term end-user refers to the ultimate operator of a piece of software.

29	ERP	Enterprise Resource Planning - refers to an integrated software application that integrates internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, customer relationship management, supply chain management, etc.
30	Full backup	Includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one full backup will be done once a week followed by differential and/or incremental.
31	Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies
32	ICT	Information Communications Technology
33	ICT Facilities	Include the network infrastructure, internet and email services, server rooms, data centres.
34	ICT System	Computer software designed to help the user to perform singular or multiple related specific business tasks. Also refers to a computer device and computer network and software managing these resources
35	ICT System Acquisition	The process that occurs from the time the decision is made to obtain a new ICT system (or replace an existing one) until the time a contract has been negotiated and signed.
36	ICT Systems Administrator	The individual who has the technical skills and the authority to ensure that the ICT Systems are in a working condition and is responsible for performing administrative duties on them.
37	ICT Systems Owner	A Manager responsible for a particular ICT System and exercises procedural and functional control over access to the system
38	ICT/IT	Information and Communication Technology is the new term used to refer to Information Technology (IT). It refers to the study or business of developing and using technology to process information and aid communications.
39	IEC	International Electro technical Commission
40	Incremental backups	Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time an incremental backup is done, this file is skipped (unless it is modified again).
41	Information	Information is interpreted data. When data is processed, organized, structured or presented in a given context so as to make it useful, it is called Information.
42	Information Processing Facilities	Any information processing system, service or infrastructure, or the physical locations housing them.

43	Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
44	Information Security Event	An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
45	Information Security Incident	an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
46	Information System	A system for generating, exchanging, storing or processing electronic data. It is also defined as a collection of hardware, software, data, people, and procedures that work together to produce quality information.
47	Integration Testing	Is a level of the software testing process where individual units are combined and tested as a group. The purpose of this level of testing is to expose faults in the interaction between integrated units.
48	ISO	International Standards organisation
49	Joint Application Development (JAD)	Refers to a system development methodology originally that involves continuous interaction with the users and different designers of the system being development. JAD centres around a workshop session that is structured and focused. Participants of these sessions would typically include a facilitator, end users, developers, observers, mediators and subject matter experts.
50	Load Testing	Is the process of putting demand on a system or device and measuring its response. Load testing is performed to determine a system's behaviour under both normal and anticipated peak load conditions. It helps to identify the maximum operating capacity of an application as well as any bottlenecks and determine which element is causing degradation.
51	Maintenance Window	The time set aside to perform normal system maintenance, such as backups, preventative.
52	Major Change	A revolutionary change accommodating sweeping architecture, approach, and implementation changes.
53	MANCO	Management Committee comprising of the Municipal Manager, all Section 56/57 managers and any member thereof
54	Military Grade Software	Software that is designed to use extreme measures to do what it is designed to do. Such software is perceived to be very good at what it does. Examples are Encryption Software, Data Deletion Software, etc.

55	Minor Change	An evolutionary incremental improvement that includes all PATCH release improvements along with fixes and enhancements that could not be accommodated without breaking backward compatibility.
56	Mobile Computer	Is any computing device that is not constrained in its location to a desktop or data centre and can be expected to be transported during its normal usage. Notebook or laptop is an example of a mobile computer
57	Patch	Is a piece of software designed to fix problems with, or update an IT System software or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.
58	Patch	A conservative incremental improvement that includes bug fixes, enhancements and new features and is absolutely backward compatible with previous Patch releases of the same Minor release.
59	Patch Management	Is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.
60	PoLP	Principle of Least Privilege describes minimal user profile or access privileges to an ICT System based on allowing access to only what is necessary for the users to successfully perform their job requirements
61	Project Management Methodology	A strictly defined combination of logically related methods and step-by-step techniques for successful planning, control and delivery of the project. It is a scientifically-proven, systematic and disciplined approach to project development and implementation while ensuring the success of current technologies and business goals. Examples are PRINCE2, Six Sigma, Critical Chain Project Management (CCPM). Other consultants custom-develop their own methodologies deriving from either one or a combination of the traditional ones
62	Quality Gate	Is a checkpoint for verification and/or validation. Implementation cannot proceed until the checkpoint has been successfully passed.
63	Rapid Application Development (RAD)	A programming system that enables programmers to quickly build working programs. In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort. Examples are Microsoft Visual Basic and Delphi.
64	Regression Testing	Is any type of software testing that seeks to uncover new errors, or regressions, in existing functionality after changes have been made to the software, such as functional enhancements, patches or configuration changes. The intent of regression testing is to assure that a change, such as a bug fix, did not introduce new bugs.
65	Remote Access Services (RAS)	The facility available to users to access information and ICT systems from a remote location, across an external telecommunications services such as Virtual Private Network

		(VPN). Remote access services enable users to work from home, access their e-mails and access their data files
66	Server Room	Is a room, usually air-conditioned, and devoted to the continuous operation of computer servers. It is usually smaller than a data centre
67	Service pack	A group of hotfixes/patches packaged into one program to address specific problems experienced with the operation of an existing program.
68	Spoof	To deceive for the purpose of gaining access to someone else's resources.
69	SQL	Structure Query Language is a database computer language designed for managing data in relational database management systems. Its scope includes data insert, query, update and delete, schema creation and modification, and data access control.
70	Standardisation	The process of developing and implementing technical standards in order to ensure that ICT delivers quality and efficient services. Sticking to one brand when purchasing hardware is one example of standardisation in ICT.
71	System	Is a group of interacting, interrelated or interdependent elements forming a complex whole that work together to achieve a particular outcome. In the computer context, a computer device, computer application/programme/software, and computer network are all examples of a system.
72	System Account	An account which has a purpose related to administration of a specific ICT System.
73	System Testing	Is a level of the software testing process where a complete, integrated system/software is tested. The purpose of this test is to evaluate the system's compliance with the specified requirements.
74	Technical Owner	The individual(s) who implemented and has/have technical knowledge and responsibility for the application. This is usually the application vendor for externally procured application, an internal official who has been extensively trained on the technical aspects of the application, or an internal technical person who was involved in the development of the in-house developed application.
75	Technical Team	Refers to the IT Section's, and the consultants where necessary, representatives in the project team. Its responsibilities are technical in nature.
76	The Municipality	Refers to Umzimkhulu Local Municipality as established in terms of the prescription.
77	Third Party	that person or body that is recognized as being independent of the parties involved, as concerns the issue in question

- Municipal Systems Act, Act 32, of 2000
- Municipal Structures Act, Act 117 of 1998
- Public Administration Management Act, Act 11 of 2014
- Municipal Finance Management Act, Act 56 of 2003
- Cobit 5
- King III Code of Good Practice
- ISO/IEC 38500
- ISO/IEC 17799-2:2005, Information technology – Code of practice for information security management
- SANS 17799-2:2003, South African National Standard: Information Security Management Systems, Part 2: Specification with guidance for use.
- Electronic Communications and Transaction Act 25 of 2002, as amended
- Electronic Communications Amendment Act 37 of 2007
- Protection Of Personal Information Act 4 of 2013
- National Archives and Records Service of South Africa Act No. 43 of 1996, as amended
- Promotion of Access to Information Act of 2000
- Public Service Corporate Governance of Information and Communication Technology Policy Framework

4. POLICY OBJECTIVES:

The objectives outlined in this policy provide general guidance in respect of various ICT Operations as included in the policy.

5. ICT SYSTEM ACQUISITIONS

5.1 POLICY PRINCIPLES

The objectives of this policy are as follows:

- To define the processes to be followed in the acquisition and implementation of all new ICT applications or replacement to existing systems by Umzimkhulu Local Municipality.
- To define the processes to be followed in the acquisition and implementation of all new ICT systems such as hardware, software, and ICT facilities in the municipality.

5.2 KEY PRINCIPLES AND GUIDELINES PERTAINING TO THE ACQUISITION OF ICT SYSTEMS/APPLICATIONS

Adherence to the MFMA Circular No. 57 and mSCOA is mandatory for acquisition of Municipal Financial Applications such as Billing, SCM, Revenue, Expenditure, HR and Payroll, Budgeting, and any other Accounting system.

- Where the provisions of this policy clash with the provisions of the circular referred to above, the provisions of the circular shall prevail.
- Prior to acquiring a new or replacement ICT application, the user department shall initiate the ICT application acquisition process by defining the problem statement, defining the scope, obtaining the project approval, and ensuring that there is a budget allocation for the proposed acquisition.
- The user department shall ensure that processes and functions to be automated by the ICT Application are aligned to the municipality's strategic objectives.
- The user department shall establish the project steering committee and appoint a project manager.
- The project team comprising the successful bidder's and the municipality's representatives shall agree on and employ a project management methodology to implement the system.
- SCM processes shall be followed in the procurement of the ICT Application.
- The accounting officer may request the State Information Technology Agency (SITA) to assist with the acquisition of ICT application.
- Data Migration is imperative where the acquisition is undertaken to replace a legacy system.
- Change management forms an integral part of the system acquisition process, particularly for major systems that encompass revenue management, financial management, supply chain management, customer relationship management, etc. and must be conducted by an experienced professional.
- Where the ICT Application's acquisition is undertaken to replace an existing system, a parallel run of the new and the legacy systems must be considered to ensure problem-free changeover.

6. ICT HARDWARE & SOFTWARE

The dependency on Information & Communication Technology (ICT) has increased progressively for the Municipality as a strategically important competitive advantage. According to the King III Report, Information systems were used as an enabler to business, but have now become pervasive in the sense that they are built into the strategy of the business.

It being imperative to comply with various prescripts and policy imperatives, a comprehensive ICT Hardware and Software Policy is crucial in providing the framework for dealing with acquisition, distribution, handling, and control of computer equipment and systems.

This Policy provides the framework for dealing with Umzimkhulu Local Municipality's computer equipment and software, and more specifically how Umzimkhulu shall:

- Acquire computer equipment
- Distribute desktop and laptop computers to users.
- Monitor users' handling of computer equipment allocated to them.

- Create standards for hardware and software for the municipality
- Maintain a computer maintenance log and equipment control list.
- Create and control a list of permitted software installed on its computers
- Maintain a control database of equipment allocations with associated paperwork

The objectives of this policy are as follows:

- To provide a framework within which Umzimkhulu Local Municipality's ICT Section shall deal with the allocation of new and/or replacement ICT hardware and software, handling, and control within the municipality.
- To provide a framework within which Umzimkhulu Local Municipality shall deal with lost or damaged computer equipment and accessories.

6.1 KEY PRINCIPLES AND GUIDELINES PERTAINING TO ICT HARDWARE OR SOFTWARE

- The ICT Manager shall analyse the need or request for ICT Hardware, decide whether the need is justified.
- The ICT Steering Committee shall establish the project steering committee and appoint a project manager for the acquisition relating to major hardware or systems.
- The Project Manager shall define the project objectives and scope analysis.
- The Project Manager shall ensure that the provisions of the ICT Operations policy are adhered to in the acquisition of hardware.
- The Project Manager must develop the Terms of Reference (TOR) for the acquisition of the hardware or systems and submit them to the Supply Chain Management (SCM) section for the preparation of Request for Proposals (RFP) or Tender.
- The Manager: SCM must follow processes per the SCM Policy and Procedures and, as agreed during the consultation sessions, to finalise the procurement process.
- The accounting officer may request the State Information Technology Agency (SITA) to assist with the acquisition of ICT hardware.
- The project team comprising the successful bidder's and the Manager: ICT shall agree on and employ a project management methodology to design and implement the ICT project.
- Change management must be an integral part of the acquisition process, particularly for major facilities upgrades that shall affect users.
- Standardisation in the municipality shall be adhered to when acquiring and/or replacing computer hardware for all users in the municipality.
 - Managers may make requests to Corporate Services manager to replace mobile computer devices with a desktop computer if the staff member does not use it for work purposes or it was provided as a temporary device.

- The mobile computer device and its accessories must be collected by the employee it is allocated to only and the employee must complete and sign the user request form.
- Desktop computer devices and accessories must be delivered by ICT to the employee it is allocated to only and the employee must complete and sign the user request form.
- The computer hardware, and its accessories, allocated to the users to perform their duties is the property of Umzimkhulu Local Municipality (inclusive of leased equipment) and will remain so until it is officially disposed of or the termination of the lease.
- It is the policy of the municipality that safeguarding of the computer equipment in the user's possession is the responsibility of such user.
- The user to which of the computer equipment is allocated is by default liable for replacement or repair of lost or damaged computer equipment. Such a user must prove absence of negligence on his/her part to transfer the liability back to the municipality.
- Lost or damaged computer equipment and/or accessories should be reported to the Manager: ICT within 24 Hours after the incident. Loss should be reported to the police and a case number presented to Manager: ICT.
- The ICT Manager shall develop, facilitate approval, and implement a Computer Hardware Replacement and a Computer Maintenance/Refresh plan.
- Mobile computer devices and their accessories must be returned to ICT only by the employee who it was allocated to, unless deceased, on employment termination and the terminated employee must complete the user exit form. Deceased employee's manager must return the computer device, and its accessories, to ICT and sign the user exit form.
- Computer devices for staff on suspension should be returned to ICT for safekeeping and the relevant form completed and signed by the HR Manager.
- Data or information on hard disk drives of all computer devices prepared for disposal shall be deleted and the computer device refreshed to make sure that municipal data or information cannot be accessed by unauthorised people. This will be controlled through a sign off per serial number by the Technical Administrator.
- Each of the municipality's boardrooms must have a ceiling or wall mounted projector to facilitate projection of presentations.

6.2 KEY PRINCIPLES AND GUIDELINES PERTAINING TO COMPUTER SOFTWARE

- Standardisation in the municipality shall be adhered to when acquiring and/or replacing computer software for all users in the municipality.

- Only permitted software, as outlined in the schedule of permitted software (available from the ICT Section), shall be installed in the computer devices allocated to users by the municipality.
- Special software that is required by a user or a group of users to perform their duties, shall be installed at a formal request authorised by the requester's HOD and approved by the Corporate Service HOD.
- Software can only be acquired by the ICT Section of Corporate Services or with the express authority of the Manager ICT.

7. ICT SERVICE DESK (HELP DESK)

The purpose of the ICT Service Desk is to establish a computer problem management system (IT Service-Desk) where all computer related problems will be recorded, tracked, and assigned.

7.1 USE OF THE SERVICE DESK

Any computer user (an employee/contractor or designate empowered by the Umzimkhulu Local Municipality to use/consume ICT resources to aid/facilitate their job.) and who requires;

- Hardware or software support
- Consumables (toner cartridges for centralized printing)
- Projectors
- Network support (new network points, etc)
- Other ICT Services

The Service Desk SOP will detail the responsibilities of the ICT Service-Desk Assistant, end-user, and ICT Support service personnel.

7.2 REQUESTING ICT SERVICE OR ASSISTANCE

The Following are 3 ways to request assistance or a service from ICT For Users of ICT services, the service desk can be accessed through the following mechanisms;

- Services requested through telephone – Extension 5030
 - This method should be used only when you are unable to use your computer and directly log the fault. A call can be made to the Service-Desk at extension 5030 and the problem reported or assistance/service requested.
- Services requested through the help-desk web interface – available on <http://helpdesk.umzimkhululm.gov.za> link
 - This is a preferred method of logging faults or requesting service and users are encouraged to use it every time they request ICT assistance.
- Services requested through email support@umzimkhululm.gov.za

7.3 OPERATING HOURS OF THE ICT SERVICE DESK

The ICT Service desk is available on;

- Monday to Friday 7:45am to 4:30pm (Excluding lunch time, 1:pm to 2:00pm)
- Saturday and Sunday, CLOSED
- Public Holidays, CLOSED

ICT helpdesk Administrators will check the logs within their sub units on a daily basis and the Manager: ICT will perform monthly reviews of all open service-desk calls with trend analysis.

8. ICT FACILITIES, ENVIRONMENTAL STANDARDS & MAINTENANCE

This policy provides the ICT infrastructure and mechanisms to help the Municipality realise its goals and objectives in setting ICT environmental standards. Access to server rooms should be justified, authorised, logged and monitored. As such, this document applies to all personnel with access to server rooms, including those entering the premises, together with staff, temporary staff, clients, vendors, visitors or any other third party.

The purpose of this policy is:

- To outline the ICT Environmental Standards.
- To ensure access to key ICT facilities is restricted to individuals who are involved in the operation and maintenance of such facilities, and is recorded.

8.1 ACCESS CONTROL

All server rooms require a manual log book in place. A weekly report of all server room entry must be extracted from the security guard by the IT security officer and reviewed by the ICT Manager.

8.2 FIRE CONTROL

- All fire exits must be kept locked and protected by a break glass system to ensure they are not used as a point of routine access or exit.
- All windows must be adequately secured to prevent access.
- Server rooms must have appropriate fire suppression systems in place which comply with all relevant health and safety legislation and have good access to appropriately signed fire exits.

8.2.2 STANDARD REQUIREMENTS

Each server room should ensure the following:

- A fire detection/Maintenance system that conforms to the above requirements.
- Detectors shall be strategically placed in room voids, floor voids and -where necessary – ceiling voids, in compliance with the design requirements of the stipulated standards.

8.3 AIR CONDITIONING

An air conditioning system that operates 24 hours a day 7 days a week must be installed in server rooms. It should be designed to keep the room to within the ICT manufacturers' recommended specifications for temperature and humidity throughout the year.

8.3.1 GENERAL

- Air conditioning equipment shall be supplied and installed by an approved contractor. It shall cater for the cooling requirements of the equipment to be housed in the facility as well as for any thermal loads generated by environmental equipment therein, by UPS systems therein, by lighting, by the introduction of fresh air, by solar radiation, by personnel and, by any other source that influences the determination of the air conditioning equipment selection.
- Equipment shall, in General, have features that allow automatic restarting in the event of a power failure unless otherwise specified. Under these conditions where multiple cooling circuits are employed, stepped or staggered re-starting of the cooling circuits shall be a mandatory requirement of this standard.
- The equipment shall comply with the relevant requirements of SABS IEC 60335-2-40, SABS 0147 and SABS ISO 5151.

8.3.2 STANDARD REQUIREMENTS

The approved contractor shall provide, as standard for each facility installation, the following:

- Air conditioning equipment of a type appropriate for the application and conforming to the minimum requirements, of this standard as well as for equipment manufacturers' recommendations.
- Air conditioning equipment of a type that is readily available and locally supported in terms of spares holding, servicing, technical back up and that is warranted for at least one year from the date of installation.

8.4 UNINTERRUPTIBLE POWER SUPPLY (UPS)

- The approved contractor shall supply, deliver and install a UPS system that is dedicated to the supply of power to critical equipment within and essential to the facility and that can, under no circumstances, suffer momentary loss of power.

- The battery backup associated with such UPS system shall be of sufficient duration to allow the ICT Administrators and ICT Technicians to implement an orderly shutdown of equipment in the event of a failure of emergency power (from the standby diesel generator) to the UPS system itself.
- **Uninterruptable Power Supply (UPS) Maintenance Services will be conducted twice per annum by an approved service provider.**

8.4.1 STANDARD REQUIREMENTS

The approved contractor shall provide, for each facility installation, the following:

- An approved current technology UPS system of a type that is readily available and locally supported in terms of spares-holding, servicing, technical back-up and that is warranted for at least one year from the date of customer acceptance.
- The standby battery supplied with such a system shall be of a maintenance-free type that is warranted for a period of between 3 – 5 years from the date of customer acceptance.

8.5 CLEANLINESS

A periodic program of specialist cleaning must be in place. The frequency of cleaning must be appropriate to the environment and include under floor and above ceiling cleaning where there is a raised floor and false ceiling. A member of the ICT Division must be present when cleaning of the room is taking place.

Staff using the room may not eat or drink in the room and must keep the room clean and free of unnecessary contamination.

9. DATA MIGRATION

Incorrect or inconsistent data can lead to false conclusions and erroneous decision-making. Data migration is the transferring of data between storage types, formats, or computer systems or applications. It is required when the Municipality changes computer systems or upgrades to new systems.

This policy defines the process to be followed by Umzimkhulu Local Municipality to migrate data from one ICT Application, usually one that is being replaced, to another.

- The Technical Team is responsible for the integrity of data and information maintained in the municipality's centralised and ICT supported applications and systems, while the User Team owns and is responsible for the accuracy of that data.
- Users are responsible for the completeness, cleanliness and accuracy of the data in applications and on the network, following agreed-upon processes and the functional requirements within user departments.

- Data Migration must form part of all the project phases. This will ensure quality and accurate data is migrated to the new system as it will be considered as and when changes are made to the new system during the implementation

THREE STAGES OF DATA MIGRATION

9.1 PRE-MIGRATION

- The User Team must perform Data Quality Analysis and Data Profiling processes to identify data to be migrated and determine its quality. Data profiling must be conducted during the project planning phase to enable an accurate estimation of the duration and cost of the migration project.
- The User Team must embark on a Data Cleansing exercise, preferably on the legacy/source system. The Technical Team may assist where technical tools can be employed to expedite the cleaning process.
- The User Team, in collaboration with the Technical Team, must undertake the Data normalisation processes.
- Data Mapping must be completed through collaboration between the User and Technical Teams.
- The Technical Team must start and complete Data Transformation process.
- Testing - After cleansing, a data set will be consistent with other similar data sets in the system. One-time conversions of data will be verified either by a representative sample or the entire data as determined by the User Team. Both the User and the Technical Teams must perform tests to ensure that all the above processes were successfully completed and that the data is ready for migration.
- The Technical Team must ensure that the necessary data backups are taken at appropriate stages of the data migration process to ensure that critical data is not lost through mistakes and unforeseen occurrences during migration process.
- The User Team must decide on whether data migration will be in phases or migrated in its entirety in one go.

9.2 MIGRATION

- This is the point within the migration process when the data is moved to the new/destination system. The Technical Team performs this task as Data migration is usually performed programmatically to achieve an automated migration, freeing up human resources from tedious tasks.

9.3 POST MIGRATION

- Testing should include comparing data in the source and destination systems to ascertain that there's reconciliation between the two.

- Quality Control - High-quality data needs to pass a set of quality criteria such as accuracy, integrity, completeness, validity, consistency, uniformity, and density. Both the User and the Technical Team must work together to ensure that the migrated data meets all the above attributes.
- Data Alignment must be undertaken to identify misplaced data, which belongs in one field, and moves it back to the correct field. Also, this process should be undertaken by the User Team in collaboration with the Technical Team.
- Data Cleanup - The User Team should identify data that has become redundant or irrelevant in the new system and Technical Team should remove such data.
- Update Data Catalogue - The Technical Team should ensure that the data catalogues and data dictionaries are updated and that they're accurate.

10. ICT CHANGE CONTROL MANAGEMENT

These Change Control Policy and Procedures are aimed to define the position of the municipality with regard to the subject of change management. It is a comprehensive statement about the intended approach to requests for system change, specifically within the Information & Communication Technology (ICT) Section and Financial Systems Section, the way in which those requests are categorized and prioritized, and the transitional process from initial request through to closure. This document provides evidence that the subject of change control is considered a business priority, and that processes must be in place to deal with Requests for Change (RFC) in a formal and structured manner.

- The first goal of the formal change control is to capture as many changes as possible, erring on the side of over-inclusion of trivial changes rather than under-inclusion of seemingly harmless changes that turn out to have a great deal of impact. In determining whether a small change (e.g. minor modification of some system configuration) should be captured in the change management process, it is presumed that any change will have an impact unless there is sufficient evidence to pass on change control.
- The common types or reasons for system changes are depicted but not limited to the following list:
 - User requests
 - Vendor recommended/required changes
 - Changes in regulations
 - Acquisition/implementation of new hardware or software
 - Hardware or software upgrades or failures
 - Changes or modifications to the infrastructure
 - Unforeseen events
 - Periodic Maintenance
 - Application modifications and enhancements
 - Patch Management

- No change request will be entertained unless it meets the following requirements:
 - All change requests, both scheduled and unscheduled, must be submitted in writing and approved by the application owner(s) affected by the change.
 - All change requests shall have an approved plan of action with milestones for implementation that provides a sequence of events or steps for implementing and releasing the change into the production environment, a roll-back plan, assigned roles and responsibilities and post implementation validation test plan.
 - A testing plan should include ICT, Financial Systems Section, business and vendors representatives where appropriate.
 - Customer notification is completed for each scheduled or unscheduled change.
 - A post change review is completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A change log is maintained for all changes. The log should contain among other items the following:
 - Date of submission and date of change
 - Owner and custodian contact information
 - Nature of the change
 - Indication of success or failure
- Change control procedures for patches may require resources and processes very different from application change control.

10.1 CHANGE MANAGEMENT RISK ASSESSMENT

Risk assessment is the responsibility of the application owner principally, but he/she should expect those working on the change, as well as peers in the change control committee, to aid and guidance. In cases where proper change control processes are followed, risks can be handled reasonably well. However, this can become a problem when change is being rushed through, especially to a production system, and the type or scope of change is new or unusual.

10.2 CHANGE MANAGEMENT REVIEWS

The purpose of periodic review is to discuss the nature of changes, notify those who may not be aware that change is imminent, and assess applications' risk and log changes in Change Control Log. A Change Control Committee should be setup, which should meet regularly to consider the following:

- Trends in changes
- Issues that have arisen regarding recent changes
- Changes made outside formal change control processes
- Assessing change impact and risk
- Policy and procedures related to the above concerns

10.3 CHANGE MANGEMENT TESTING

Assessing risk and testing are critical components to change control. It is the responsibility of all change requesting managers to document impact and risk and to identify testable components as part of a brief testing plan. In short, testing generally consists of the following:

- Integration Testing - performed by the programmers or independent testers
- Systems Testing - performed by the programmers or independent testers
- Acceptance Testing - performed by the requesting user(s)
- Load, Stress and Failure Mode Testing - only necessary for major changes to the system, is performed by the programmers or independent testers
- Security - performed by programmers or independent testers as well as requesting users.
- Regression - performed by programmers or independent testers and requesting users.
- Documentation and Training Assessments - performed by change manager and requesting manager.

10.4 CHANGE MANAGEMENT PROCESSES

The change control process follows the entry-task-validation-exit (ETVX) model, and is depicted below:

10.4.1 ENTRY STAGE

The change control process is initiated when there is a requirement to make a change. Change is defined as any of the following:

- New system - application, operating system, database, hardware platform or infrastructure.
- Major upgrade to an existing system - version release, new or upgraded components and/or subsystems (hardware or software), database schema reorganization, etc.
- Minor upgrades to an existing system - patches, modifications to existing scripts or additional scripts (batch, shell, SQL, etc.), minor database schema reorganization (dropping columns, adding or modifying constraints, triggers and stored procedures, etc.) and changes that are transparent to end users (i.e. Graphic User Interface).
- Maintenance to any system that has dependencies with the system being managed internally requires that the Manager Responsible for Financial Systems opens a change request to document the maintenance being performed on the inter-dependent system. The vendor representative for the application to be changed is responsible for initiating change control. However, since the change will affect the second application, the Manager Responsible for Financial Systems or vendor representative responsible for the system will also initiate a change request. This provision will ensure that the scope of the required impact analysis will extend to all systems that are affected by the change. It will also ensure that each system owner and vendor remain cognizant of any change or maintenance activity that affects their system.

The following are the minimum entry steps that must be met before the process can move to the task stage:

- Release notes, build analyses, installation manuals and any other documentation that is needed to correctly test and install the product (hardware or software).
- Test results from Quality Assurance (User Acceptance Test and/or pre-production/staging).
- Operational requirements, such as special training, maintenance window considerations, etc.

10.4.2 TASKS STAGE

- Perform an impact analysis. The outcome is a completed impact analysis.
- Develop planning package. The outcome is a description of change and why change is being made (including benefits and how the change will create value for the users), how the change will affect users during the implementation (scheduled start and end time, impact on maintenance window and service level objectives) implementation plan, roll-back plan, roles and responsibilities, notifications, quality assurance plan.
- Provide operational requirements, implementation plan and change request to application owner, Manager(s) Responsible for ICT and Financial Systems for review and approval.
- Application owner approves the change.
- Manager(s) Responsible for ICT and ERP review(s) the change control package for completeness.
- IT Steering Committee reviews change requests quarterly.
- Change is implemented in accordance with implementation plan.
- Change action is closed out as complete.

10.4.3 VALIDATION STAGE

The following are checkpoints in the change control process:

- All entry steps will be checked for accuracy and completeness by the Manager(s) Responsible for ICT and Financial Systems.
- The Application owner will review and approve the change request before proceeding.
- The Manager(s) Responsible for ICT and Financial Systems will review and approve the change request before proceeding.
- The Manager Responsible for ICT will review the implementation plan and change request for accuracy and completeness.
- The change will successfully pass all post implementation validation test checkpoints before the change is released into production, else the change will be rolled-back.
- In the event of a roll-back there will be a root cause analysis performed and responsibility for eliminating the root cause and, when applicable, developing a process improvement plan will be assigned to individual(s) by cognizant authority. The

change request will also be cancelled and resubmitted after the root cause has been determined and eliminated.

10.4.4 EXIT STAGE

- The change is successfully released into the production environment or cancelled and resubmitted depending on validation checkpoints above.
- After a change is successfully released into the production environment the Manager Responsible for ICT will close out the change request as completed.

11. WEBSITE MANAGEMENT

The Municipal website serves as an integral part of the communications strategy. It allows easy access to relevant information, serves as a tool for community participation, improves stakeholder involvement and facilitates stakeholder monitoring and evaluation of municipal performance. Umzimkhulu Local Municipality will use its official municipal website to serve long-term, seasonal, new, and potential residents and other visitors: connecting them to local government, community information, events, and important factual information.

The website will include:

- Easy to find and retrieve municipal information such as meeting schedules, official announcements, minutes, policies, plans, bylaws, emergency contact information, etc.
- Council information
- Access to complete and clear answers to frequently asked questions.
- Contact information for Officials and Departments
- Links to important and relevant websites.

12.1 WEBSITE COMPLIANCE

The Municipality will publish the following information in line with the MFMA regulations on its website;

No	Documents published on the Municipality's website
1	The previous annual report (2014/15)
2	All current performance agreements required in terms of section 57(1)(b) of the Municipal Systems Act 2015/16 and resulting scorecards
3	All service delivery agreements 2015/16
4	All long-term borrowing contracts 2015/16
5	An information statement containing a list of assets over a prescribed value that have been disposed of in terms of section 14 (2) or (4) during 2015/16
6	Contracts were agreed upon in 2015/2016 to which subsection (1) of section 33 apply, subject to subsection (3) of that section

No	Documents published on the Municipality's website
7	Public-private partnership agreements referred to in section 120 were made in 2015/16
8	All quarterly reports were tabled in the Council in terms of section 52 (d) during 2015/16
9	Copies of the draft and final <u>Medium Term Revenue and Expenditure Framework</u> / (i.e. <u>Municipal Budgets</u>) in the prescribed format as per Section 17 of the Local Government: Municipal Finance Management Act, 2003 with the following supporting documents:
10	Resolution Approving the budget of the municipality;
11	Resolution and municipal tariffs of the budget year;
12	any proposed amendments to the municipality's <u>integrated development plan</u> following the annual review of the integrated development plan in terms of section 34 of the Municipal Systems Act;
13	any proposed amendments to the budget-related policies of the municipality;
14	particulars of the municipality's investments;
15	particulars of all proposed new municipal entities which the municipality intends to establish or in which the municipality intends to participate;
16	Any <u>request for a formal written quotation</u> which is likely to be in excess of R30000 must be advertised for at least 7 (seven) days on the municipal official website and an official notice board as applicable. (Mini tender)
17	Tenders awarded per month
18	particulars of any proposed allocations or grants by the municipality to-
19	(i) other municipalities;
20	(ii) any municipal entities and other external mechanisms assisting the Municipality in the exercise of its functions or powers;
21	(iii) any other organs of state;
22	the proposed cost to the municipality for the budget year of the salary, allowances and benefits of-
23	(i) each political office-bearer of the municipality;
24	(ii) councilors of the municipality; and
25	(iii) the municipal manager, the chief financial officer, each senior manager of the municipality and any other official of the municipality having remuneration package greater than or equal to that of a senior manager;
	any prescribed budget information on municipal entities under the sole or shared control of the municipality;

No	Documents published on the Municipality's website
26	Measurable performance objectives for revenue from each source and for each vote in the budget, taking into account the municipality's integrated development plan;
27	a projection of cash flow for the budget year by revenue source. broken down per month;
28	Minutes of Umzimkhulu LocalMunicipal Council

12.2 WEBSITE MANAGEMENT AND GOVERNANCE

- No advertising will be allowed on Umzimkhulu Local Municipality's website to avoid any conflict of interest issues.
- Ensure continuity of operations during emergencies; develop emergency procedures.
- Avoid redundant content on the site.
- Create operating procedures to manage the site and all the functions that support it: everyone in the governance structure knows and understands the policies and procedures.
- Establish responsibilities for each person that is involved with the website: everyone should know and understand their roles and be accountable for their content areas.
- Management controls identified to ensure the website and web operations are protected from fraud, waste, abuse and mismanagement, and the controls are reviewed regularly.
- Website will be fully-accessible .
- A website task team comprising of the Manager ICT and Website champions representing each Department of the Municipality will be convened once per quarter to continually review content.
- The system owner of the Municipal website is the Communications Unit of the Municipality and all content will be vetted by Communications officer and approved by the municipal manager prior to being uploaded on the website .**(with the exception of AG Compliance documents approved by respective HODs .i.e. SCM,Policies, etc.**
- **The Communications officer is responsible for the publication of content to the official Umzimkhulu Local Municipality Facebook page.**
- The address of the official website is www.umzimkhululm.gov.za
- **Departments will appoint departmental Website Champions to ensure integrity and posting of content on the website, attend and input at Website Champions meetings.**

12.3 CONTENT MANAGEMENT GUIDELINES

- Content for the following functional areas of the website must be vetted by communication officer and approved by the Municipal Manager before posting on the live website;
 - Home Page
 - About Us
 - Council
 - Departments
 - Contact Us
- Content for the following functional areas of the website must be approved by the HODs before posting on the live website;
 - Access to Info – Annual Reports
 - Access to Info – Performance Agreements
 - Access to Info – Quarterly Reports
 - Access to Info – IDP
 - Access to Info – SDBIP
- Content for the following functional areas of the website must be approved by the HOD before posting on the live website;
 - Opportunities – New t
 - Opportunities – Tender Opening Register
 - Tenders – all areas
- Content for the following functional areas of the website must be vetted by the Manager Budget and approved by HOD before posting on the live website;
 - Downloads – Budgets & Budget Policies
- Content for the following functional areas of the website must be approved by the General Manager Corporate Services before posting on the live website;
 - Downloads – Council Minutes
 - Jobs

System owners of content approval should ensure the following prior to approval;

- Assurance that content is current and accurate.
- Organize content based on audience needs.
- Write for the Web in plain language.
- Documents posted as PDFs
- Use appropriate image resolutions and format for the web.

12. LICENCING MANAGEMENT

The Umzimkhulu Local Municipality will centralise all ICT Licence management within the ICT Section of the Corporate Services Department, inclusive of all software and software licences. This will include procedures for corporate licence ownership and management, procurement, Policy: ICT Operations Policy

distribution, recovery, and systems decommissioning. The ICT Section will establish and manage an approved software list as well as detect and take steps to remove unapproved software installed within the Municipality.

14.1 KEY PRINCIPLES AND GUIDELINES PERTAINING TO LICENCING MANAGEMENT

The objective of this policy is to establish a consistent approach to identifying and mitigating risk as well as reduce costs through the centralisation of the ownership and management of all of the Municipality's software.

The benefits of centralised licencing management include;

- greater control over the installation and deployment of software
- the establishment of a centralised registration system that captures information on all installed software
- the establishment of a single area for software accountability within the Municipality

13. BACKUPS AND RESTORES

The dependency on Information & Communication Technology (ICT) has increased progressively for organizations as a strategically important competitive advantage. According to the King III Report, Information systems were used as an enabler to business, but have now become pervasive in the sense that they are built into the strategy of the business.

It being imperative to comply with various prescripts and policy imperatives, a comprehensive Backup and Restore Policy and Procedures is crucial in providing the guideline to keeping the municipality's data/information safe and secure. This policy and procedures explain the steps to backup and restore Information & Communication Technology services if any 'disaster' disables any of Umzimkhulu Local Municipality Information & Communication Technology equipment. A disaster includes events like fires, natural disasters, riots. It also includes malicious viruses, hacking or any activity that stops the normal working of the systems. The steps taken to preserve key data/information in the advent of a 'disaster' are also included in this document. Also the unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery.

This Policy and procedures provide the framework for the backup and restore of Umzimkhulu Local Municipality's data/information, and more specifically how Umzimkhulu shall implement the policy and procedures to:

- Backup data/information.
- Conduct regular restores.
- Restore data/information when required.

The objectives of this policy are as follows:

- To provide a framework within which Umzimkhulu Local Municipality performs backup and restore of data/information.
- Explains the steps to backup and restore Information & Communication Technology services if any 'disaster' disables any of Umzimkhulu Local Municipality Information & Communication Technology equipment.

15.1 KEY PRINCIPLES AND GUIDELINES PERTAINING TO DATA BACKUP & RESTORE

- ICT recognises that the backup and maintenance of the municipality's data and server are critical to the viability and operations of the municipality's departments.
- The Manager: ICT has a responsibility to ensure that backup of all municipal files, servers and databases are performed as outlined in the procedures.
- Backup of municipal files, server and databases shall occur every day after regular business hours.
- Backup media shall be stored off site for a period of 30 days retention.
- Backup schedules shall be kept, reviewed and signed off by the delegated IT personnel on a daily basis.
- Backup schedules shall be reviewed and signed off by the responsible official: ICT on a monthly basis.
- Testing of backup restore shall be performed at least once every quarter.
- Backup restore testing schedules shall be kept, reviewed and signed-off by the delegated IT personnel each time they're carried out.
- Backup restore testing schedules shall be reviewed and signed-off by the Manager: ICT every three months.
- Requests for backup restore should be authorised by the Manager: ICT and ICT System Owner where a system is involved.
- Operating System and Database Logs shall be retained as part of the monthly backup for a period of twelve (12) months.

15.2 DATA BACKUP & RESTORE PROCEDURES

All official Umzimkhulu Local Municipality data is stored on one backup server linked to the SAN storage.

The offsite backup solution uses the redstor backup solution that runs the backup to centralized backup server and then at schedule time will synchronize with Munsoft centurion data centre.

The backup software to be used to control the backup processes is Redstor Backup pro

15.3 BACKUP CONTENT

The content of data backed up varies from server-to-server. The following is the primary data that will be backed up:

- Domain Control Files (System Files for the network control servers).
- File Servers (Data Files designated by the respective data owners who made sure that the data they generated and documents created are stored on the servers).
- Applications/Systems (Business system files and other selected software installed on the server).
- Exchange Servers (All email servers from the different sites).
- SQL Servers (Specific Databases relating to core systems)

15.4 BACKUP SCHEDULING

The following applications are backed up in terms of the procedures below:

<u>ITEM</u>	<u>SCHEDULE</u>	<u>PROTECTION SERVER</u>
<u>Munsoft</u>	<u>Daily, Monthly Offsite</u>	
<u>VIP</u>	<u>Daily, Monthly Offsite</u>	<u>VEEAM</u>
<u>DOMAIN CONTROLLER/Active Directory</u>	<u>Daily, Monthly Offsite</u>	<u>VEEAM</u>
<u>EXCHANGE</u>	<u>Daily, Monthly Offsite</u>	<u>VEEAM</u>
<u>SYSAID server</u>	<u>Daily, Monthly Offsite</u>	<u>VEEAM</u>
<u>EDMS</u>	<u>Daily, 2 week retention</u>	<u>VEEAM</u>
<u>GIS</u>	<u>Daily, 2 week retention</u>	<u>VEEAM</u>

15.5 BACKUP TYPES

- Full backups and Incremental backups
- Daily incremental backups take place on a **14 day** rotation.
- Monthly backups occur on the last calendar day of the month.
- Ad-hoc snapshot backups are taken and used specifically for emergency, roll-back planning and remediation purposes.

15.6 BACKUP TESTING AND RESTORE

Users that need files restored must submit a request to the help desk.

The file restoration requisition should be completed and should include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was destroyed, this process has to be authorised by the appropriate supervisor of the requesting employee.

System Restore

Should there be a system failure where an emergency restore is required, the system administrator may restore the necessary data and then later document the restore and test thereof and have the documentation approved by the supervisor of the affected section.

All application data and User Data will be restored according to the restore procedure to test and ensure that the backed up data is still in working condition and that backup was 100% successful.

Testing

The ability to restore data from backups shall be tested as per the application/system set rules. All tests conducted will be logged on the test schedule document.

Restore tests are to be performed as per agreed schedule of service and the identified personnel as per schedule of service is to sign off on success or failure thereof.

In the event of test failure, the failure must be logged in the appropriate incident tracking system and Root Cause Analysis provided. This RCA will be used to prevent repeat of failure. Once the incident is resolved, the restore test must be run to successful completion.

15.7 DATA RETENTION

- Financial systems data will be stored for a period of 5 years.

14. MUNICIPAL STRUCTURE, ROLES, AND RESPONSIBILITIES

17.1 THE MUNICIPAL COUNCIL

Provide political leadership and strategic direction through:

- Determining policy and providing oversight
- Take an interest in the Corporate Governance of ICT to the extent necessary to ensure that a properly established and functioning Corporate Governance of ICT system is in place in the municipality to leverage ICT as an enabler of the municipal IDP.
- Assist the municipal manager to deal with intergovernmental, political and other ICT-related municipal issues beyond their direct control and influence
- Ensure that the municipality's organisational structure makes provision for the Corporate Governance of ICT.

17.2 THE MUNICIPAL MANAGER

- Provide strategic leadership and management of ICT
- Ensure alignment of the ICT strategic plan with the municipal IDP
- Ensure that the Corporate Governance of ICT is placed on the municipality's strategic agenda

- Ensure that the Corporate Governance of ICT policy, charter, and related policies for the institutionalism of the Corporate Governance of ICT are developed and implemented by management.
- Determine the delegation of authority, personal responsibilities, and accountability to the management with regards to the Corporate Governance of ICT.
- Ensure the realisation of municipality-wide value through ICT service delivery and management of municipal and ICT-related risks.
- Ensure that appropriate ICT capability and capacity are provided and a suitably qualified and experienced Governance Champion is designated
- Ensure that appropriate ICT capacity and capability are provided and that a designated official at a management level takes accountability for the management of ICT in the municipality
- Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of ICT system e.g. ICT Steering Committee.

17.3 THE ICT STEERING COMMITTEE, RISK, AND AUDIT COMMITTEE

- Assists the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.
- Reviews change requests for impact to business operations based on degree of risk associated with the requested change.
- Approves or rejects change requests based on the outcomes of the business impact risk review.
- On approval, the chairperson signs-off the change request for implementation.
- Composed of Manager Responsible for ICT, IT Officer, Manager Responsible for ERP/Applications Administrator, Committee Secretary, Affected Application Owner(s)), Affected Service Provider Representative (invited).
- Reviews change control packages for accuracy and completeness.
- Reviews change requests for impact to business operations based on degree of risk associated with the requested change, trade-off between accepting known defects and deferring the change.
- Accepts and recommends to IT Steering Committee the change requests based on the outcomes of the business impact risk review.
- Conducts periodic review of change control procedures and trends.

17.4 RESPONSIBILITIES OF MANAGER: ICT

- Provides technical advice and assistance to the user department and the project team during the planning, implementation, and post implementation phases.
- Ensures availability of the ICT infrastructure required to successfully acquire and implement the ICT application.

- Takes over the management of technical support, licensing, and maintenance upon the successful implementation of the acquired ICT application.
- On the acquisition of ICT Hardware:
- Defines the problem statement or the identified need to clearly define the problems that will be resolved or the need that will be fulfilled by the acquisition of the ICT Hardware or facility.
- Ensures that such hardware or facility shall positively contribute to the attainment of the municipality's strategic objectives.
- Conducts an extensive evaluation of the hardware or facility's requirements and risk assessment.
- Prepares a submission for the acquisition of the new or replacement hardware or facility and obtain approval from the ICT Steering Committee.
- Obtain budgetary approval and institutional support through the ICT Steering committee.
- Assumes responsibility of the ICT facility or hardware post implementation and provides for maintenance and support of the same.
- Ensures adherence to this policy and the attached standards when acquiring hardware and software for new staff or when replacing existing computer hardware and software.
- Manages the distribution of new or replacement computer hardware, accessories and software as stated in this policy.
- Implements all requests approved by the General Manager: Corporate Services as explained above.
- Updates the computer control register on acquisition of new or replacement ICT hardware and submits the updated the control register to the municipality's Treasury Department.
- Reports all reported damaged or lost computer equipment to General Manager: Corporate Services for any investigation necessary to determine if damage or loss were caused negligence.
- Enforces change control policy for all IT systems and applications related change requests.
- Conducts periodic review of the policy and procedures, with the assistance of the Manager Responsible for ERP, at least every twelve months and making any changes required to reflect changes to business and technical objectives.
- Signs-Off on change requests approved by the Change Control Committee.
- Presents the change control packages to the IT Steering Committee for approval.
- Reviews the results of software patching tests conducted by the System Administrators.
- Reviews and approved patch implementation schedules presented by ICT System Administrators

- Oversees the implementation of software patches.
- Oversees the post deployment review of the effects of patches applied and decided whether to roll back.

17.5 RESPONSIBILITIES OF FINANCIAL ADMINISTRATOR

- Responsible and accountable for complying with change control policy.
- Inform application owners of the proposed change(s) so that they can be aware of the possible impact to or affecting their applications.
- Review change control requests for accuracy and completeness and sign-off on them.
- Maintain a log of open, pending and closed change requests.
- Participates in the Change Control Committee meetings to present application changes to the same.

17.6 RESPONSIBILITIES OF VENDORS AND CONTRACTORS

- All service providers sponsored by, or performing services for the municipality through the IT and ERP sections are required to adhere to the policy and follow the process and procedures set forth in this document.
- Review or develop technical impact analyses.
- Develop implementation and roll-back plan.
- Are invited to the Change Control Committee meetings to provide technical and system knowledge capacity.

17.7 RESPONSIBILITIES OF USER DEPARTMENT

- Works with the Manager: ICT, or delegated ICT representative, to formulate detailed requirements for the ICT application.
- Defines the problem statement or the identified need. This should clearly define the problems that will be resolved or the need that will be fulfilled by the acquisition of the ICT application.
- Identifies processes and functions that require extensive automation and defines how the ICT application will improve operational efficiency for the department.
- Conducts an extensive evaluation of the system requirements, feasibility analysis, and risk assessment with the assistance of the Manager: ICT, or delegated ICT representative.
- Determines the goals and objectives of, and prioritises the ICT application's requirements.
- Evaluates and select from the available information system acquisition options, which are:
 - Commercial Off the Shelf System (COTS),
 - Developing the IT application in-house
 - Contracting a system developer to develop the required IT application

- Leasing the required IT application from an Application Service Provider (ASP)
- Purchasing a custom application from a vendor
- In deciding on any of the above options, the user department must consider a value-versus-risk matrix to determine which option(s) can be chosen to implement the application.
- Prepares a business case document for the acquisition of the new or replacement system and obtain approval from the relevant management committees.
- Obtain budgetary approval and institutional support through the relevant management committees
- Works with the Manager: ICT, or delegated ICT representative, to develop the Terms of Reference and submit them to the Supply Chain Management (SCM) section for the preparation of Request for Proposals (RFP).
- Appoints its representatives to form part of the project implementation team.
- Participates and takes ownership of data migration processes in the replacement of a legacy application.
- Assumes responsibility of the ICT Application post implementation.

17.8 RESPONSIBILITIES OF COMPUTER USERS

- Ensures that the computer devices allocated to him/her is kept in good condition and that any accessories supplied with the computer device are kept and returned with the latter on termination of the user's employment or during computer hardware replacement.
- Ensures that the software installed in the computer equipment is authorised as outlined in this policy and attached standards.
- Ensures the safety of the computer equipment provided to him/her and that he/she reports, in writing, any damage or loss of computer equipment to his/her manager.
- Saves all work-related documents on My Documents, Individual, Section or Departmental shared drives.
- Shall, unless deceased, personally return the mobile computer he/she's been using on termination of employment and sign the computer return form.
- Initiates and submits change requests
- Signs off on the change where appropriate
- Participates in user testing, pre-deployment testing and post deployment testing.

17.9 RESPONSIBILITIES OF ICT STEERING, MANCO, RELEVANT PORTFOLIO AND EXECUTIVE COMMITTEES

- The ICT Steering committee reviews and approves technical scope of the system to be acquired.

- MANCO committee reviews and approves the entire acquisition plan and recommends the business case document, i.e. need to acquire a new system document, to the relevant portfolio committee.
- The Portfolio committee reviews and approves the business case document and recommends it to the Executive committee for final approval.
- Executive committee approves the business case document for the acquisition process to begin.

17.10 RESPONSIBILITIES OF MANAGER: SUPPLY CHAIN MANAGEMENT

- Advises the user department on the proper procurement process to be followed in the acquisition of the new ICT application.
- Prepares the bid documents and oversees the entire SCM process until procurement of the ICT Application is completed.

17.11 RESPONSIBILITIES OF PROJECT MANAGER

- Employs the agreed upon project management methodology to implement the acquired ICT application from planning to production.
- Defines project objectives and scope analysis.
- Adheres to the approved Change Control policy to manage new and out-of-scope requirements.
- Employs the services of a professional Change Manager to conduct proper change management to affected staff for mission critical systems as explained in sections 6.1.9 and 6.2.10 of this document.
- Collaborates with the user department to perform Data Migration tasks as outlined in the Data Migration Policy and Procedures.

17.12 RESPONSIBILITIES OF MANAGER: INTERNAL AUDIT

- Plays a consulting role in advising on the implementation of internal controls for both the business processes and the ICT application being implemented.
- Plays a monitoring and support role during the entire implementation process.
- Reviews, recommends changes and provides an appraisal on the adequacy and effectiveness of internal controls that have been implemented on the acquired application before it goes to production.

17.13 RESPONSIBILITIES OF APPLICATION OWNERS

- Responsible and accountable for complying with change control policy and the integrity of applications and systems under his/her responsibility.
- Initiates change requests, approves change requests made by end-users/functional users.

- Notifies Manager Responsible for ERP of change requirements.
- Ensures that all requirements associated with change requests have been met.

17.14 RESPONSIBILITIES OF SECTION MANAGERS/UNIT HEADS

- Initiates the requests for provision of ICT Mobile hardware to staff from level section manager and unit heads to motivate for such request.
- Initiates the requests for replacement of ICT Mobile hardware with desktop computer to staff using motivated for mobile ICT hardware equipment and give reasons.
- Initiates request for new computer equipment for staff reporting to them using the Computer Request form.
- Initiates request for non-standard software, as per attached standards, and motivate for its installation on a user's or group of users' computer equipment.
- Submits any of the motivated requests, referred to above, to their General Manager or Head of Department for approval.
- Reports to Manager: ICT any damage or loss of any computer equipment used by him/her or reported by the staff under his/her supervision.

17.15 RESPONSIBILITIES OF HEADS OF DEPARTMENTS

- Authorises or rejects requests submitted by Section Managers as detailed above.
- Submits approved requests to General Manager: Corporate Services

17.16 RESPONSIBILITIES OF MANAGER CORPORATE SERVICES

- Reviews, approves, request further information, or rejects requests submitted by other General Managers or Heads of Departments per section 7.1.2 above.
- Submits approved requests, per section 7.1.2 above, to Manager: ICT for implementation.
- Initiates investigation to determine whether negligence caused the reported damage or loss of computer equipment and makes the final decision

17.17 RESPONSIBILITIES OF NETWORK ADMINISTRATOR

- Determine what the current patching level of all software, applications, network and server operating systems.
- Watch out for alerts and new patch releases by the application or system vendors and trusted third parties.
- Download and test patches and updates using test servers.
- Develop and submit patch implementation schedules to the Manager: ICT for approval.

- Deploy the software patches upon successful testing and approval of software patch implementation.
- Conduct post deployment of patches and submit the report to the Manager: ICT.

15. POLICY APPLICATION

This policy applies to all users of computing facilities provided by the municipality, including but not necessarily limited to councillors, officials, contractors, consultants, temporary staff, students undergoing experiential training and authorised guests. It covers Acceptable Use, Personal Use and Prohibited Use of the municipality's facilities, encompassing but not restricted to:

- Network infrastructure, including (but not exclusively) cable or wireless, together with network servers, firewall, connections, switches and routers;
- Network services, including (but not exclusively) internet access, web services, e-mail, wireless, messaging, telephony and facsimile services;
- Computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, Personal Digital Assistants (PDAs), servers, printers, scanners, disc drives, monitors, keyboards, tablets and pointing devices; and
- Software and databases, including (but not exclusively) applications and information systems, virtual learning and videoconferencing environments, laboratories, software tools, information services, electronic journals and e-books

16. EXCEPTIONS TO THE PRINCIPLES OF THIS POLICY

Exceptions to this policy will only be granted under the following conditions:

- Compliance would adversely affect the ability of the service to accomplish a mission critical function.
- Compliance would have an adverse impact on the service provided or supported by the application or resource.
- Compliance cannot be achieved due the incapability or system limitations of the ICT System.
- An exception request form to this policy will be produced and implemented.

17. MONITORING AND EVALUATION

This ICT Operations Policy shall be monitored and evaluated by the Municipal Manager and regular monitoring reports submitted to the operational Management Committee Meeting, ICT Steering Committee, Sound Governance and Human Resources Portfolio Committee, Executive Committee and Full Council Meetings.

18. COMMENCEMENT

This version of the ICT Operations Policy is a consolidation of several policies with the inclusion of new content. The following policies are at adoption of the ICT Operations Policy considered defunct and are replaced with the ICT Operations Policy;

- Backup and Restore Policy
- ICT general project management framework
- ERP and Other Applications Change Control Policy and Procedure
- ICT Systems Acquisition Policy
- ICT Hardware and Software Policy
- Helpdesk User Guide
- ICT Helpdesk Manual
- Data Migration Policy and Procedures

19. AMENDMENT AND/OR ABOLITION

This policy may be amended or repealed by the Municipality through a Council Resolution.

20. COMPLIANCE AND ENFORCEMENT

Violation or non-compliance with this policy will give a just cause for disciplinary steps to be taken.

21. POLICY REVIEW

This Policy will be reviewed annually to ensure applicability and relevance.

22. APPEAL PROCESS/ GRIEVANCE PROCEDURE

The policy must also state what will happen if one of the users thereof is not satisfied or there is a violation with the implementation process.

Records of Approval

Meeting	Date	Resolution
Policy		
ICT Operations Committee		Consultation comments
ICT Steering Committee		Consultation comments
Sound Governance and Human		Recommended to EXCO

Resources Portfolio Committee		
EXCO		Recommended to Council
Council		ADOPTED
POLICY REVIEW		
Policy Review Committee		Consultation comments
ICT Steering Committee		Consultation comments
Sound Governance and Human Resources Portfolio Committee		Recommended to EXCO
Local Labour Forum		Consultation Comments
EXCO		
Council		