ANNEXURE A

ICT POLICIES

2026/2027

ICT CHANGE MANAGEMENT POLICY

1 July 2026

Table of Contents

1. INTRODUCTION

a) Information systems and technology is increasingly used as an enabler of the business of the municipality in fulfilling its strategic mandate. Due to the nature of the mandate municipality, there are both critical business and peripheral information systems in use.

b) These information systems facilitate the delivery of processes, human intervention with these processes and the information carried within them. Inevitably the business-critical information systems have grown to become a core engine of the business of the municipality.

c) Information and communication technology (ICT) change management institutes a discipline and quality control in the form of planning, evaluation, review, approval, communication, implementation, documentation and post-mortem activities in the form of rules and processes.

d) The Change Management Policy objectives are:
   1.4.1 To protect the computing environment from uncontrolled changes;
   1.4.2 To restrict service disruptions caused by necessary changes to defined low-use hours;
   1.4.3 To minimize the occurrence of unintended effects during the implementation of necessary changes.

e) This positions the municipality to facilitate efficient and effective control of changes and the introduction of new technology and solutions in the ICT environment. The change management processes, approval structures and controlled implementation ensure the protection of the business of the municipality.

f) This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:
   1.6.1 The municipality is unable to render normal information system-based services;
   1.6.2 Inability to retrieve or access historical information required to serve the public;
   1.6.3 Decrease in productivity reverting back to manual transactions;
   1.6.4 Degrading management practices;
   1.6.5 Reduction in turnaround times;
   1.6.6 Lapse or breach in information security;
   1.6.7 Productivity losses; and
   1.6.8 Exposure to reputational risk.

2. LEGAL FRAMEWORK

a) The following legislation, amongst others, was considered in the drafting of this policy:
   - 2.1.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
   - 2.1.2 Copyright Act, Act No. 98 of 1978;
   - 2.1.3 Electronic Communications and Transactions Act, Act No. 25 of 2002;
   - 2.1.4 Municipal Finance Management Act, Act No. 56 of 2003;
   - 2.1.5 Municipal Structures Act, Act No. 117 of 1998;
   - 2.1.6 Municipal Systems Act, Act No. 32, of 2000;
   - 2.1.7 National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
   - 2.1.8 Promotion of Access to Information Act, Act No. 2 of 2000;
   - 2.1.9 Protection of Personal Information Act, Act No. 4 of 2013;

3. SCOPE

a) The Change Management Policy applies to the production, test and development environments and applies to:
   - 3.1.1 To all staff and line function units;
   - 3.1.2 ICT-related service providers;
   - 3.1.3 ICT department and users of electronic information resources within the municipality;
   - 3.1.4 It addresses planned changes to all forms of authorised information and communication systems;
   - 3.1.5 Upgrades, including software and operating patches;

4. CHANGES TO ICT RESOURCES

a) The IT Manager is responsible for ensuring that the Change Management Policy is implemented and maintained. Changes to ICT information resources shall be managed and executed according to a formal change control process. The control process will ensure that the changes proposed are:
   - 4.1.1 Documented - Document (process, culture, cloud, application and back office configuration and architectural implications) the change and any review and approval information.
   - 4.1.2 Planned - Plan the change, including the implementation design, scheduling, test plan (where possible) and roll-back plan.
   - 4.1.3 Approved - Obtain approval from the CFO as needed.
   - 4.1.4 Communicated - Communicate change with the appropriate parties.
   - 4.1.5 Implemented - Implement the change.

5. APPLICATION FOR AND APPROVAL OF CHANGE REQUEST

To fulfil this policy, the following rules shall be adhered to:

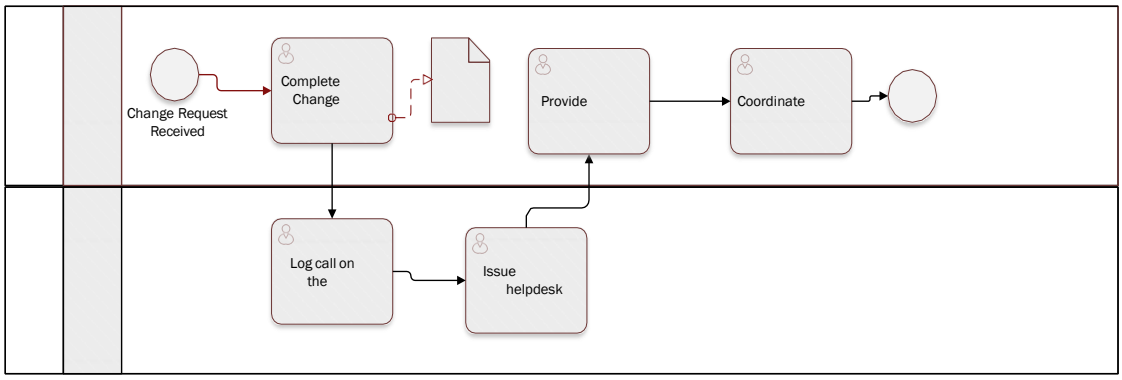
a) Standard Changes

5.1.1 A change request shall be handled according to the following procedure:

a) The requestor completes the change request form (Annexure A);
b) The completed form is provided to the municipal contact person for the specific information system i.e. SOLAR – Senior Operator and Resourcelink – Manager Financial Services;
c) Contact person logs the change request on the ICT helpdesk and obtains helpdesk reference number;
d) The contact person provides approval for the roll-out of the change;
e) The contact person monitors that the change was applied.

5.1.2 In the case of standard changes that are approved by the CMC (See Annexure B), which will be revised as and when required but a least annually, the change request form is not completed. The responsible person will log a call on the helpdesk and coordinate that the change is applied.

5.1.3 The following process applies:



5.1.4 In terms of Control is a completed and approved change requests availible where applicable and the Chairperson of the CMC validates that appropriate controls are applied on a six monthly basis.

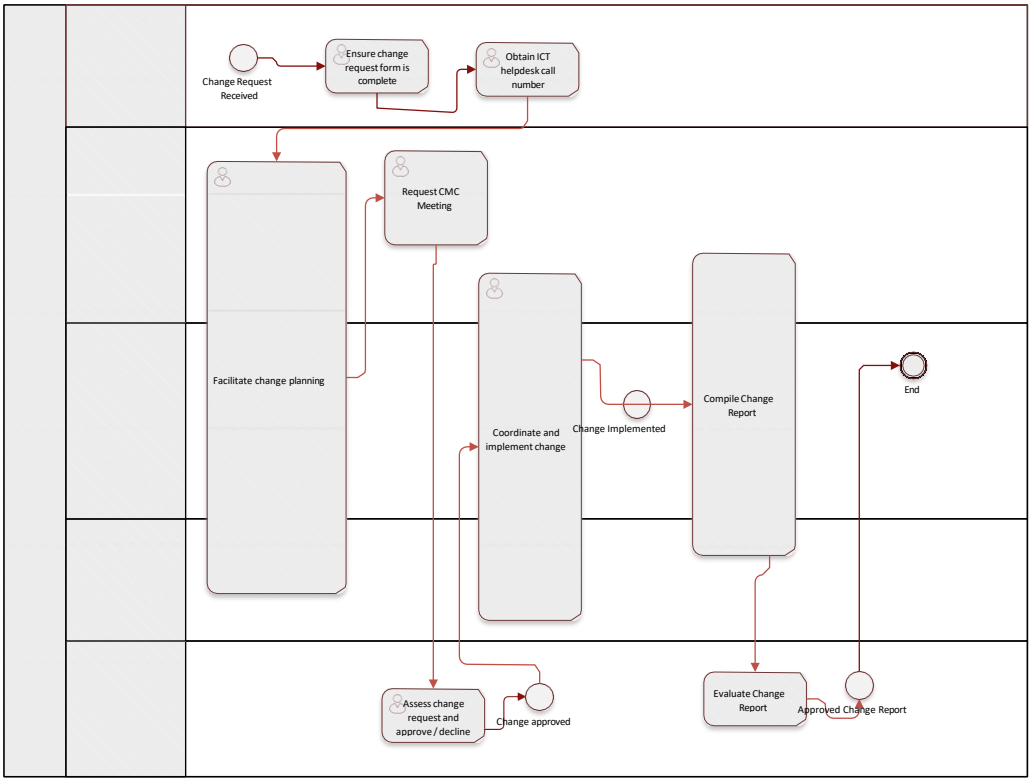
5.2 Significant Changes

5.2.1 A chanage request shall be handled according to the following procedure:

a) The requestor completes the change request form (Annexure A);

b) The completed form is provided to the municipal contact person for the specific information system i.e. SAMRAS –Manager Financial Services;
c) Contact person logs the change request on the ICT helpdesk and obtains helpdesk reference number;
d) The call is routed to the Chairperson of the CMC (Senior Manager ICT) to arrange ad-hoc change management meetings;
e) Senior Manager ICT routes request to the appropriate official to plan and present the change at the CMC;
f) Responsible official facilitates planning of the change;
g) The change impact, risk of the change, the change implementation plan and process for roll-back serves at the CMC for evaluation and approval;
h) The CMC shall consider risk and impact with regards to the change request and approve or disapprove;
i) The relevant official coordinates implementation;
j) Change report is drafted; and
k) CMC accepts change report.

5.2.2 The following process applies:



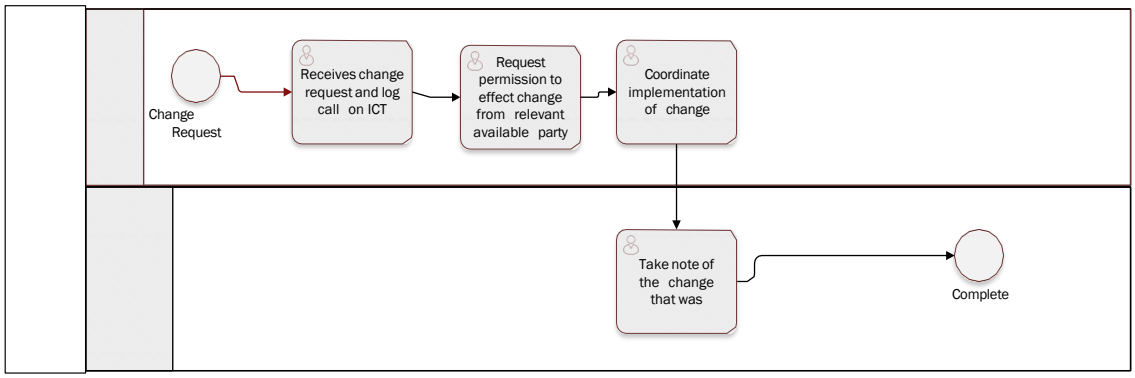
5.2.3 In terms of control the completed and approved change requests and reports must be available.

5.3 Emergency Changes

5.3.1 A change request shall be handled according to the following procedure:

a) Requestor completes the change request form.
b) The municipal contact person logs the change request on the ICT helpdesk and obtains helpdesk reference number.
c) The municipal contact person request approval to affect change from the relevant party verbal, short message service or e-mail.
d) The municipal contact person coordinates the implementation of the request.
e) The municipal contact person sends an e-mail to support@drakenstein.gov.za to log a call on the helpdesk.
f) The helpdesk issues a call number.
g) The municipal contact person routes the request, call number and relevant documentation to the chairperson of the CMC to organise and ad-hoc meeting.
h) At the CMC meeting the relevant information for the completed request is noted and where necessary feedback provided to all roll players.

5.3.2 The following process applies:



5.3.3 In terms of control, completed and approved change requests and reports are available.

6. CHANGE CLASSIFICATION

7.2 All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on business and ICT operations according to the following guidance:

6.1.1 Standard Change – A low-risk change with well-understood outcomes that is regularly made during the course of normal business. A Standard change follows pre-determined processes, is pre-approved by the CMC and may be made at the discretion of the municipal representative, Senior Manager ICT, Executive Manager Corporate Services or Municipal Manager. Standard changes will be revised on an annual basis. A list of standard approved changes is attached as Annexure B.

6.1.2 Significant Change – A significant change is one that has results in a change of mission critical information systems (Financial and Human Resource and other core systems), it involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Because of the ability to affect downstream or upstream business services, any proposed significant change must be authorised by the CMC.

6.1.3 Emergency Change – this is similar to a significant change, but must be executed with utmost urgency. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps, but any emergency change must be approved by the Staff and/or Line Function Senior Manager, Senior Manager ICT, Executive Manager Corporate Services or the Municipal Manager.

6.1.4 Classified Changes - the CMC can, from time-to-time update the list of standard changes as deemed necessary.

6.1 All changes, except standard changes, should be planned and reflect as a minimum the following:

6.1.1 What will be changed;
6.1.2 Role-players and their responsibilities;
6.1.3 When will the change take place;
6.1.4 Implementation plan;
6.1.5 Version control;
6.1.6 Rollback plan; and
6.1.7 Impact on the ICT Continuity Plan.

7 Change request information required:

7.1 Infrastructure:

7.1.1 Infrastructure refers to all identifiable elements of the Swellendam domain. This includes data links (terrestrial and radio), domain technology (servers, routers and switches), database and software

systems that facilitates the provisioning and operations of the domain and any other technology implemented that provisions the service to the user-base and where allowed service providers. These change requests should take the following into consideration:

a) Description of the environment within which the change is requested;
b) Impact on technology, processes and standard operating procedures;
c) Impact on skills and competency requirements;
d) Purpose of the change requested;
e) Risk of the change requested; and
f) Impact on the ICT Business Continuity Plan.
g) Change control form is attached as Annexure A.

7.1.2 Application, cloud back-end information change request encompasses any information/application systems (regardless of where it is housed) that are used to provide presentation layer interfaces to the user and includes the appropriate back- end systems used to manage the data of these (i.e. databases and middleware). In this regard the change request should take the following in consideration:

a) Information system in which the change is requested;
b) Purpose of the information system;
c) Business processes impacted and its implications;
d) How the change will relate to change in business processes;
e) Business culture change requirements and management;

7.1.3 For systems housed in-house: Related information system change requirements in terms of: database systems, application systems, integration with other systems, infrastructure and underlying operating system requirements;

7.1.4 For systems housed in the cloud: Integration with other systems, infrastructure and underlying operating system requirements; and

a) Impact on the ICT Business Continuity Plan.
b) Change control form is attached as Annexure A.

7.2 Cloud Based Information System

7.2.1 These are information systems that are housed by the service provider within its private hosting space (cloud) and are managed through a service level agreement between the staff and line function and the supplier. These suppliers are expected to inform the municipality of a

change that will be performed and when the change will be implemented. Furthermore, these kind of change requests will only serve to inform the CMC of the intention of the supplier to perform the change. In this regard, the following should be taken into consideration:

a) What the business uses the information system for;
b) Impact on business process and how it will be changed; and
c) Business culture change requirements and management.
d) Change control form see attached as Annexure A.

8 COMPOSITION OF THE CHANGE MANAGEMENT COMMITTEE (CMC)

8.1 The CMC shall comprise of the following members:

8.1.1 Senior Manager ICT (Chair Person);
8.1.2 ICT Governance and Administration Manager;
8.1.3 Information Systems Manager;
8.1.4 Operations and Support Manager;
8.1.5 Staff and/or Line Function Senior Manager or Manager;
8.1.6 Where a service level agreement (SLA) is involved, a representative of the service provider; and
8.1.7 Any other role player that may be co-opted from time-to-time.

9 TESTING OF PROPOSED CHANGES

9.1 Changes shall, where possible, be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation. This is done in order to minimise the impact on business and information system security. Where requested changes cannot be tested the CMC should be satisfied that the proposed changes do not pose an unnecessary risk to the business functionality or ICT infrastructure and information systems environment.

9.2 A change register shall be maintained by the Senior Manager: ICT.

10 CONTROLS

10.1 The following controls apply:
10.1.1 List of standard changes shall be approved by the CMC;
10.1.2 All change requests are recorded in the change control register;

10.1.3 The change control register will be signed by the Manager ICT Governance and Administration on a quarterly basis and Senior Manager ICT six monthly.

11 COMPLIANCE

11.1 Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary action in accordance with the Disciplinary Code.

12 RETENTION OF CHANGE MANAGEMENT DOCUMENTATION

12.1 Change management documentation will be retained in accordance with the requirements of the relevant information system.

ICT DATA BACKUP AND RECOVERY POLICY

1 July 2026

Table of Contents

1. ABBREVIATIONS

"AD" refers to the active directory.

"ICT" refers to Information Communication Technology.

"IT" refers to Information Technology.

"ICTCOM" refers to the ICT Steering Committee.

"SWDM" refers to Swellendam Municipality.

"*Municipality*" refers to the Swellendam Municipality.

"email" refers to electronic mail.

"MM" refers to the Municipal Manager.

"Site Manager" refers to the service provider appointed to provide technical support.

"Manager ICT Services" refers to the Head of the ICT Services Division.

"CFO" refers to the Chief Financial Officer or Director Financial Services.

"SCM" refers to Supply Chain Management.

"HR" refers to Human Resource Management.

"Users" refers to Councillors, Employees, End Users, Interns, Temporary Staff Members and Contract Workers.

"Manager" refers to the Head of each Division.

"Network Devices" refers to computers and devices interconnected by communications channels that facilitate communications among users.

"IR" refers to the Information Resources.

"SLA" refers to Service Level Agreement.

"Workstations" refers to computers, laptops, printers and photocopiers.

"VPN" refers to Virtual Private Network.

"ISO" refers to International Organization for Standardization.

"POPIA" refers to the Protection of Personal Information Act.

2. PURPOSE OF THE POLICY

2.1 Information security is becoming increasingly important to the SWDM, driven in part by changes in the regulatory environment and advances in technology.

2.2 Information security ensures that the SWDM ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as the unauthorised disclosure or incorrect processing of data.

2.3 The Backup procedure is responsible for ensuring that all municipality data stored on approved systems within the SWDM environment is recoverable in the event of accidental loss or damage.

2.4 The purpose of the policy is to protect the SWDM data. This policy seeks to outline the data backup and recovery controls for Municipal employees to ensure that the data is correctly and efficiently backed up and recovered in line with best practices.

2.5 The policy must ensure that the SWDM conforms to a standard backup and recovery control process in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, and service efficiency.

2.6 In addition, it seeks to define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.

3. LEGISLATIVE FRAMEWORK

3.1 The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

3.2 The following legislation, among others, was considered in the drafting of this policy:

- 3.2.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- 3.2.2 Copyright Act, Act No. 98 of 1978
- 3.2.3 Electronic Communications and Transactions Act, Act No. 25 of 2002
- 3.2.4 Minimum Information Security Standards, as approved by Cabinet in 1996
- 3.2.5 Municipal Finance Management Act, Act No. 56 of 2003
- 3.2.6 Municipal Structures Act, Act No. 117 of 1998
- 3.2.7 Municipal Systems Act, Act No. 32, of 2000
- 3.2.8 National Archives and Record Service of South Africa Act, Act No. 43 of 1996
- 3.2.9 National Archives Regulations and Guidance
- 3.2.10 Promotion of Access to Information Act, Act No. 2 of 2000
- 3.2.11 Promotion of Administrative Justice Act, Act No. 3 of 2000
- 3.2.12 Protection of Personal Information Act, Act No. 4 of 2013
- 3.2.13 Regulation of Interception of Communications Act, Act No. 70 of 2002
- 3.2.14 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

3.3 The following internationally recognised ICT standards were leveraged in the development of this policy:

- 3.3.1 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- 3.3.2 Control Objectives for Information Technology (COBIT) 5, 2012
- 3.3.3 ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- 3.3.4 King Code of Governance Principles IV, 2009

4 USER AWARENESS

4.1 Every councillor, employee, contractor and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of

adhering to it when using the Municipality's computers, networks, data and other information resources. Each user is responsible for reporting any suspected breaches of this policy's terms to the Manager: ICT Services.

4.2 The contents of this policy will be made available through presentations to all staff members and all those who attend must sign an attendance register and/or email and/or place it on the SWDM Network.

5 SCOPE

5.1 This ICT Data Backup and Recovery Policy have been created to guide and assist the SWDM to align with internationally recognised best practices, regarding data backup, recovery controls and procedures. This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

5.2 The policy applies to everyone in the SWDM, including its service providers and consultants. This policy is regarded as crucial to the effective protection of data, of ICT systems of the SWDM.

5.3 SWDM must develop their own Data Backup and Recovery controls and procedures by adopting the principles and practices put forward in this policy.

6 DATA BACKUP STANDARDS

6.1 Critical data, which is critical to the SWDM, must be defined by the municipality in consultation with ICT and must be backed up.

6.2 Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site).

The medium will dictate when scheduled. (To be implemented when disaster recovery site is established).

6.3 Data restores must at least be tested quarterly.

6.4 Procedures for backing up critical data and the testing of the procedures must be documented by the ICT Services Division. These procedures must include, as a minimum, for each type of data and system:

6.4.1 A definition of the specific data to be backed up;

6.4.2 The type(s) of backup to be used (e.g. full backup, incremental backup, etc.);

6.4.3 The frequency and time of data backup;

6.4.4 The number of generations of backed-up data that are to be maintained (both on-site and off-site);

6.4.5 Responsibility for data backup;

6.4.6 The storage site(s) for the backups;

6.4.7 The storage media to be used;

6.4.8 Any requirements concerning the data backup archives;

6.4.9 Transport modes; and

6.4.10 Recovery procedure of backed-up data.

7 DATA BACKUP SELECTION

7.1 All data and software essential to the continued operation of the SWDM, as well as all data that must be maintained for legislative purposes, must be backed up.

7.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.

7.3 The application owner, together with the ICT, will determine what information must be backed up, in what form, and how often.

8. BACKUP TYPES

8.1 Full backups should be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time.

8.2 Once a month, a full backup should be stored off-site. This statement will be subject to the review of the ICT Disaster Management Policy and is updated with input from System Administrators, Line Managers and Municipal operations. (Currently, only SAMRA'S is stored offsite. Once disaster Recovery is implemented the rest of the backups will be stored offsite.)

8.3 Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.

8.4 If a system requires a high degree of skill to recover from backup, consideration must be given to making full images of such servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.

8.5 For monitoring purposes, the ICT Manager must create a summary of backup types, along with their advantages, disadvantages and frequency.

9. BACKUP SCHEDULE

9.1 Choosing the correct Backup Schedule:

9.1.1 Backup schedules must not interfere with day-to-day operations. This includes any end-of-day operations on the systems.

9.1.2 A longer backup window might be required, depending on the type of backup.

9.2 Frequency and time of data backup:

9.2.1 When the data in a system changes frequently, backups need to be taken more frequently to ensure that data can be recovered in the event of a system failure.

9.2.2 Immediate full data backups are recommended when data is changed to a large extent or the entire database needs to be made available at certain points in time. Regular, as well as event-dependent intervals, need to be defined.

9.3 Previous versions:

9.3.1 The ICT Manager should determine the number of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location.

9.3.2 Annual, monthly and weekly backups must be retained at the Backup and Disaster Recovery location. Weekly, Monthly and Annual backup media may be re-used to take new backups. (To be implemented when disaster recovery site is established.)

10. DATA BACKUP PROCEDURES

10.1 The ICT Manager in collaboration with the CFO must choose between automated and manual backup procedures based on their requirements and constraints. Both procedures are in line with best practices.

10.2 The ICT Manager in collaboration with the CFO must choose between centralized and decentralized backup procedures based on their requirements and constraints. Both procedures are in line with best practices.

10.3 The ICT Manager must submit quarterly to the ICTCOM the register of backups taken, the frequency and which procedure was done and where the backups were stored.

11. STORAGE MEDIUM

11.1 When choosing the data media format for backups, it is important to consider the following:

11.1.1 Time constraints around identifying the data and making the data available;

11.1.2 Storage capacity;

11.1.3 Rate of increasing data volume;

11.1.4 Cost of data backup procedures and tools vs. cost if restored without backup;

11.1.5 Importance of data;

11.1.6 Life and reliability of data media;

11.1.7 Retention schedules; and

11.1.8 Confidentiality and integrity.

11.2 Should high availability be required, a compatible and fully operational reading device (e.g. tape drive, CD, DVD) must be obtainable on short notice to ensure that the data media is usable for restoration even if a reading device fails.

12. DATA BACKUP OWNER

12.1 The SWDM should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, so to ensure segregation of duties and responsibilities and to mitigate the risk of systems and data losses.

12.2 The ICT Manager has the discretion in collaboration with the CFO, to assign ICT staff members to ensure each backup schedule is maintained. (To be implemented when disaster recovery site has been established)

13. OFFSITE STORAGE SITE

(To be implemented once a site is established)

13.1 Data backups must be stored in two locations:

13.1.1 One on-site, or in close proximity, with current data in a machine-readable format in the event that operating data is lost, damaged or corrupted; and

13.1.2 An off-site location, to additionally provide protection against loss to the primary site and on-site data.

13.2 Off-site backups must be a minimum of 6 kilometres from the on-site storage area to prevent a single destructive event from destroying all copies of the data.

13.3 Should high availability be required, additional backup copies may be securely stored in the close proximity to the ICT system (within the data centre or secure vault).

13.4 Minimum requirements are to store the monthly and/or yearly backup sets off-site.

13.5 The site used for storing data media off-site must be physically secure and safe.

13.6 Receipts of media being collected and delivered must be kept for record-keeping purposes and must be signed by ICT personnel in attendance.

13.7 Should an off-site media set be required to perform a restore, the data media must be returned to the offsite facility for the remainder of the applicable retention period.

13.8 All data media used to store information must be disposed of in a manner that ensures the data is not recoverable.

13.9 This will be implemented once an off-site storage site has been identified.

14. TRANSPORT MODES

14.1 When choosing the transport mode for the data (logical or physical), it is important to consider the following:
- 14.1.1 Time constraints;
- 14.1.2 Capacity requirements; and
- 14.1.3 Security and encryption.

15. RETENTION CONSIDERATION

15.1 Data should be retained in line with current legislative requirements, as defined in sections 19 and 20 of this document.

15.2 The minimum retention of backups is as follows:

- 15.2.1 A full system backup will be performed weekly, where possible or not longer than two (2) weeks. Weekly backups must be saved for a full month.
- 15.2.2 The last full backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled by the backup system.
- 15.2.3 Monthly backups must be saved for one year, at which time the media will be reused or disposed of.
- 15.2.4 Yearly backups must be retained for five (5) consecutive financial years and will only be run once a year at a predetermined date and time.
- 15.2.5 Differential or Incremental backups will be performed daily. The retention of Daily backups should be determined by the ICT Manager. Daily backup media will be reused once this period ends.

16. RECOVERY OF BACKUP DATA

16.1 Backup documentation must be maintained, reviewed and updated by the ICT Manager periodically to account for new technology, business changes,

and migration of applications to alternative platforms. This includes, but is not limited to:

16.1.1 Identification of critical data and programs; and

16.1.2 Documentation and support items necessary to perform essential tasks during a recovery process.

16.2 Documentation of the restoration process must include:

16.2.1 Procedures for the recovery

16.2.2 Provision for key management should the data be encrypted.

16.3 Recovery procedures must be tested at least quarterly and Disaster Recovery procedures must be tested at least yearly.

16.4 Recovery tests must be documented and submitted to the CFO and ICTCOM.

17. BACKUPS IN RECORD MANAGEMENT

17.1 The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the SWDM functions, activities and transactions. The detail of these requirements can be found in:

17.1.1 The National Archives and Records Service of South Africa Regulations; and

17.1.2 Other applicable municipal policies, may include policies relating to Records Management, Employee Information, Internet and E-mail Usage, Web Content Management, Social Media Content and Document Imaging/Management in the Municipality.

17.2 The Records Manager is responsible for the implementation of sound records management principles and records disposal schedules for the SWDM. The

Records Manager is also responsible for maintaining the retention periods indicated on the file plan and disposal schedule.

17.3 The ICT Manager must liaise and work closely with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

17.4 Backups are not ideal, but not excluded, as a means of electronic record and e-mail retention for the prescribed periods. It is difficult to implement a proper file plan using backup media and therefore it is difficult to arrange, retrieve and dispose of records. Archiving solutions may be considered for electronic records and email retention.

17.5 The role of backups in records management is more suited as a means to recover electronic records management systems and e-mail systems in the event of a disaster or technology failure.

17.6 The ICT Services Division is responsible for the following when backing up electronic records or e-mails that are regulated under the National Archives and Records Service of South Africa Act:

17.6.1 Backups must be made daily, weekly and monthly;
17.6.2 Backups must cover all data, metadata, audit trail data, operating systems and application software;
17.6.3 Backups must be stored in a secure off-site environment and no backup and backup system must be stored or hosted outside the borders of the Republic of South Africa.
17.6.4 Public records being backed up must conform to the municipal File Plan;
17.6.5 Backups must survive technology obsolescence by migrating them to new hardware and software platforms when required. An additional option to ensure that data can be read in the future is to store electronic records and e-mails in a commonly used format e.g. PDF or XML.
17.6.6 The backup and retrieval software/system must also be protected to be available in the event of a disaster;

17.6.7 The integrity of backups must be tested using backup test restores and media testing.

17.7 The ICT Manager must implement measures to ensure that systems prevent the deletion of electronic records or e-mails.

17.8 The ICT Manager in consultation with the Records Manager must implement the most practical method to retain e-mails e.g. file inside e-mail application, transmit to document management solution, transfer to e-mail archiving solution, save to shared network drive, print to paper etc.

17.9 Officials are responsible for filing e-mails. It is the discretion and responsibility of the sender or receiver to file e-mails.

17.10 The Records Manager, in conjunction with the ICT Manager, must create awareness among Officials of the importance of e-mail as public records. This could include, but is not limited to:

17.10.1 E-mails must be properly contextualised and meaningful over time;
17.10.2 Subject lines are very important and must be descriptive;
17.10.3 Auto-signatures must be used and shall contain full details of the sender; and
17.10.4 Attachments must be filed into the file plan in the document management system before it is attached to the e-mail.

17.11 The ICT Manager must ensure that the e-mail system is set up to capture the sender and the recipient(s), and the date and time the message was sent and/or received.

17.12 The ICT Manager and Records Manager may dispose of any electronic records and e-mails if retention is not required under any Act or General Disposal Authority.

18. GENERAL RULES FOR RETENTION PERIODS

18.1 The National Archives provides the primary considerations when defining retention periods of electronic records and e-mails.

18.2 This supports the goals of the Promotion of Administrative Justice Act, Act. No. 3 of 2000, which is to ensure that public records are available as evidence to ensure that administrative action is lawful, reasonable and procedurally fair.

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.2.1	National Archives and Record Service of South Africa Act, Act No. 43 of 1996	Public records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions.	Records may not be disposed of unless written authorisation has been obtained from the National Archivist or a Standing Disposal Authority has been issued by the National Archivist against records classified against the file plan.
Nr	**National Archive Act, Regulations and Guidance**	**Item**	**Retention Period**
18.2.2	General Disposal Authority PAP1Disposal of personal files of localauthorities	Personal case files of local authorities	At the discretion of the Municipality, taking into consideration any special circumstances.
18.2.3	General Disposal Authority No. AE1 for the destruction of ephemeral electronic records andrelated documentation	Electronic records with no enduring value	16 Categories of records. Refer to AE1 for details.
18.2.4	General Disposal Authority No. AT2 on the destruction of transitory records of all governmental bodies	Electronic records not required for the delivery of services, operations, decision-making or to provide accountability	Refer to AT2 for details.

18.2.5	Managing electronic records in governmental bodies Policy, principles and requirements Managing electronic records in governmental bodies Metadata requirements	E-mails, and attachments therein, must be retained if they: • Are evidence of Municipal transactions; • Approve an action, authorize an action, contain guidance, advice or direction; • Relate to projects and activities being undertaken, and external stakeholders; • Represent formal business communication between staff; or • Contain policy decisions.	E-mails fall into one of the 4 categories above and must be retained as such.

18.3 The Municipal Finance Management Act, No 56. of 2003, Section 62 1)b) states that Municipal records must be retained in the manner prescribed by legislation. However, the Act does not specify retention periods.

18.4 National and Provincial retention periods for financial records are prescribed within Treasury Regulations, Regulation 17 to the Public Finance Management Act, No. 1 of 1999, Section 40(1)(a). For the purposes of this policy, the Treasury Regulations, Regulation 17, will be used as guidance only without intervening in National Archivist legislation, regulations and guidance.

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.4.1	Treasury Regulations, Regulation 17	Internal audit reports, system appraisals and operational reviews.	10 years

18.4.2	Treasury Regulations, Regulation 17	Primary evidentiary records, including copies of forms issued for value, vouchers to support payments made, pay sheets, returned warrant vouchers or cheques, invoices and similar records associated with the receipt orpayment of money.	5 Years
18.4.3	Treasury Regulations, Regulation 17	Subsidiary ledgers, including inventory cards and recordsrelating to assets no longer held or liabilities that have been discharged.	5 Years
18.4.4	Treasury Regulations, Regulation 17	Supplementary accounting records, including, for example, cash register strips, bank statements and timesheets.	5 Years
18.4.5	Treasury Regulations, Regulation 17	General and incidental source documents not included above, including stock issue and receivable notes, copiesof official orders (other than copies for substantiating payments or for unperformed contracts), bank deposit books and post registers.	5 Years

18.5 Per the Treasury Regulations, Regulation 17(2), financial information must be retained in its original form for one year after the financial statements and audit report has been presented to the Council.

18.6 Financial information may be stored in an alternative form, after expiry of one year from submission of the financial statements to the Council, under the following conditions:

18.6.1 The records must be accessible to users. This requires data referencing, a search facility, a user interface or an information system capable of finding and presenting the record in its original form.

18.6.2 The original form may have reasonable validations added, which is required in the normal course of information systems communication, storage or display.

18.7 The Electronic Communication and Transaction Act, No 25 of 2005 regulates the storage of personal information:

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.7.1	Electronic Communication and Transaction Act, No 25 of 2005	Personal information and the purpose for which the data was collected must be keptby the person who electronically requests,collects, collates, processes or stores the information.	As long as the informationis used, and at least 1 year thereafter.
18.7.2	Electronic Communication and Transaction Act, No 25of 2005	A record of any third party to whom the information was disclosed must be kept for as long as the information is used.	As long as the information is usedand at least 1 year thereafter.
18.7.3	Electronic Communication and Transaction Act, No 25of 2005	All personal data which has become obsolete.	Destroy

18.8 The Protection of Personal Information Act, No. 4 of 2013 ("POPI") regulates theretention of personal information:

Nr	National Archive Act, Regulations and Guidance	Item	Retention Period
18.8.1	Sections 9 to 18	Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views,	Do not collect or retain unless the person has been given notice and express consent is obtained. Exceptions apply. Personal information may not be

		preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears nextto other personal information or if the name itself would reveal personal information about the person.	retained for longer than agreed with the person unless the retention of the record is required by law. (This principle applies to all items in this table. The retention ofitems that follow is expressly prohibited unless exceptions apply.)
18.8.2	Sections 6, 34 to 37	Children's information	Destroy unless exceptions apply e.g. establishment or protection of a right of the child.
18.8.3	Sections 6 & 28	Religious or philosophical beliefs	Destroy unless exceptions apply e.g.to protect the spiritual welfare of a community.
18.8.4	Sections 6 & 29	Race or ethnic origin	Destroy unless exceptions apply e.g. protection from unfair discriminationor promoting the advancement of persons.
18.8.5	Sections 6 & 30	Trade union membership	Destroy unless exceptions apply e.g.to achieve the aims of trade union that the person belongs to.
18.8.6	Sections 6 & 31	Political persuasion	Destroy unless exceptions apply e.g.to achieve the aims of a political institution that the person belongs to.
18.8.7	Sections 6 & 32	Health or sex life	Destroy unless, exceptions apply e.g. provision of healthcare services, special support for pupils in schools, childcare or support for workers.
18.8.8	Sections 6 & 33	Criminal behaviour or biometric information	Destroy unless exceptions apply e.g. necessary for law enforcement.

19. BACKUP STRATEGY

19.1 The below table is used to guide on the backup strategy. Any deviations from the strategy must be reported by the ICT Manager to the CFO.

19.2 A register of backups taken in line with the below table must be kept by the ICT Manager and be submitted monthly to the CFO and quarterly to the ICTCOM.

Data Set	Full Backup			Differential Backup	Incremental Backup
	Monthly	Weekly	Yearly	Daily	Daily
Financial Sytems	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
HR Systems (Payroll, T&A, Leave, etc.)	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
File and Print Services	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
Business Enablers (Mail, eDirectory, AD, SQL, etc.)	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday
Supporting Material (Application installation files)	Last weekend in the month	Last day of the week	The weekend after Financial Year End	Monday to Friday	Monday to Friday

20. BACKUP DESIGN PRINCIPLES

20.1 The Municipality will need to standardise its backup solution and backup medium(s) across all sites to implement the policy. The backup medium(s) may include data replication to another site.

20.2 The following design principles and requirements have been taken into consideration in informing the Backup Architecture Design inclusive of with integrated application awareness, and is in response to several business requirements, legal constraints and technical issues:

20.2.1 Provide a unified and integrated data management solution to protect the production systems at all pertinent municipal sites and data centres;

20.2.2 Protection of the Directory and Domain Controllers;

20.2.3 Protect File Servers data on Physical Servers;

20.2.4 Protection of the Email Server;

20.2.5 Protection of the MSSQL;

20.2.6 Protection of the SharePoint Data;

20.2.7 Protection of Virtual Machines hosted on VMWare (VMware backups to be made via SANMode and Live sync to be used for Critical Virtual Servers, when required);

20.2.8 Maintain copies of backup data on disk or USB drive. (SAMRAS);

20.2.9 Maintain warm Virtual Machine warm disaster recovery site (To be implemented when disaster recovery site is established);

20.2.10 All Backup Clients will be protected by local media agents at Head Office and the DR site with the Disk Library in combination with deduplication. (To be implemented when disaster recovery site is established);

21. SYSTEMS PROTECTION STRATEGY

21.1 Windows File System

21.1.1 Windows File System Agent will be used to protect File System & System State dataon local disks of Physical Servers.

21.1.2 Weekly Synthetic Full and Daily Incremental backup schedules will be implemented.Paths & Shares to be protected will be specified.

File System Protection:	Physical Servers (Windows File System)
Data Protection Summary	▪ Daily deduplicated Inc backup ▪ Weekly Synthetic(DASH) Full
Service Account Requirements (Permissions / Rights)	▪ Local Administrator ▪ Read\Write Access to Shared Folders

21.2 Unix\Linux File System & NFS

21.2.1 Unix/Linux File System Agent will be used to protect File System & System State data on local disks of Physical Servers.

21.2.2 Weekly Synthetic Full and Daily Incremental backup schedules will be implemented. Paths & Shares to be protected will be specified.

File System Protection:	**Physical Servers (Unix\Linux File System)**
Data Protection Summary	• Daily deduplicated Inc backup • Weekly Synthetic(DASH) Full
Service Account Requirements (Permissions / Rights)	• Local Administrator • Read\Write Access to Shared Folders

21.3 Active Directory and eDirectory

21.3.1 The Microsoft Active Directory Domain of SWDM is hosted on a Domain Controller. Domain Controllers are Virtual Machines in VMWare environment and Domain Controller is hosted at the Swellendam Data Site.

File System Protection:	Domain Controller
Data Protection Summary	• Daily Full with Active Directory Agent

21.4 Microsoft SQL Server

21.4.1 The SWDM has MSSQL Servers, which are both Standalone MSSQL Servers and host instances & databases. The Backup Schedule will include a Daily Incremental and Transaction Log backup daily for all MSSQL Instances.

File System Protection:	**MSSQL Databases**
Data Protection Summary	• Daily Incremental Backup • Transaction Log Backup daily
Service Account Requirements (Permissions / Rights)	• Local Administrator • SQL Admin • System Account

21.5 VMWare Infrastructure

21.5.1 The SWDM has VMWare ESX hosts in cluster configuration in the Swellendam domain, managed by a single vCenter server per site, which needs to be protected with Virtual Server Agents. All the VMs are to be protected with VM Level backup.

VMWare Protection:	**VM Guests utilising VHD-based disks(VM Level backups)**
Data Protection Summary	• Daily deduplicated Incremental backup • Weekly DASH Full
VMWare Requirements (Permissions / Rights)	User accounts for • Local Administrator • VMWare Administrator role

22. BREACH OF THIS POLICY

22.1 Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract must be reported to the Director of Financial Services which will assess its level of severity. Appropriate disciplinary action or punitive recourse may be instituted against any user who contravenes this policy.

22.2 Actions may include, but are not limited to:

22.2.1 Revocation of access to Municipal systems and ICT services;

22.2.2 Disciplinary action in accordance with the SWDM disciplinary procedures;

22.2.3 Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or

22.2.4 Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

23. POLICY REVIEW

23.1 The policy shall be reviewed annually by the ICT Steering Committee.

ICT DISASTER RECOVERY PLAN

1 July 2026

Table of Contents

1. INTRODUCTION

This ICT Disaster Recovery Plan is a step in the ICT development process that provides the necessary business continuity demands of Swellendam Municipality in case of a disaster. This will summarize the strategies being developed for the Swellendam Municipality and contains the strategic intentions and guidelines on Business Continuity Management in the municipality.

Therefore, Swellendam Municipality's initial strategy is to look for any potential problems within the ICT environment and take corrective action. Swellendam Municipality intends to address those issues that can be resolved to keep the exposure within acceptable levels. If a disaster occurs, Swellendam Municipality must be able to continue with its ICT activities with minimal disruption.

This ICT Disaster Recovery Plan will ensure that effective Business Continuity Management is implemented and maintained so that the municipality can recover in the event of a major disruption, crisis or disaster which threatens the ongoing existence of the municipality.

2. LEGISLATION

The following legislation, among others, was considered in the drafting of this policy/plan:

a) Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
b) Copyright Act, Act No. 98 of 1978;
c) Electronic Communications and Transactions Act, Act No. 25 of 2002;
d) Minimum Information Security Standards, as approved by Cabinet in 1996;
e) Municipal Finance Management Act, Act No. 56 of 2003;
f) Municipal Structures Act, Act No. 117 of 1998;
g) Municipal Systems Act, Act No. 32, of 2000;
h) National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
i) Promotion of Access to Information Act, Act No. 2 of 2000;
j) Protection of Personal Information Act, Act No. 4 of 2013;
k) The Disaster Management Act, Act No. 57 of 2002; Regulation of Interception of Communications Act, Act No. 70 of 2002; and
l) Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

3. PURPOSE

The purpose of this ICT Disaster Recovery Plan - strategy is to provide contingency arrangements and services that will meet the ICT recovery demands of the Swellendam Municipality to be used in cases of a disaster.

This Plan will ensure that the interests of the municipality are secured in the event of major damage to the municipality's operations. The strategy shall support the ongoing governance, Compliance and risk initiatives and challenges faced by the municipality. This document will reflect the up-to-date status of the strategy adopted and will be reviewed and maintained regularly.

The ICT Business Continuity Strategy shall encompass ICT, data communications and voice communications equipment.

4. OBJECTIVES

The objectives of a formalised ICT Business Continuity Management strategy document are as follows:

a) To ensure compliance with regulatory, statutory and legal requirements relative to business continuity for the Swellendam Municipality;

b) Provide business-critical services to clients throughout a disaster or major incident;

c) Minimise potential financial loss or legal liabilities;

d) Utilise limited resources (human and technological) more effectively during the response, resumption and recovery phases, and

e) Ensure the ICT Service Continuity strategy aligns with the Swellendam Municipality's risk appetite and meets the required minimum standards but does not deliver a solution that is excessive and unwarranted.

5. INCIDENT VERSUS DISASTER

Municipal functions are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, hardware failure, denial of access to the building, partial damage to offices) to severe (e.g. equipment destruction, fire).

Vulnerabilities may be minimised or eliminated through technical, management, or operational solutions as part of the municipality risk management effort. However, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service disruption by focusing on effective and efficient recovery solutions.

The table below helps differentiate between Incidents and Disasters to assist in determining when the plan should be activated and when normal recovery will suffice.

Scenario	Possible causes	Impact	Recovery strategy
Destructive loss of a building.	Fire, explosion/ bomb, sabotage, flood, structural failure and natural Disasters.	• Almost all hardware, office infrastructure, equipment and non-electronic files are destroyed; and • Interruption of all business activities.	Activate the BCP /ICT DRP.
Loss of infrastructure.	Loss of power, flood, lightning, theft.	• Major loss of ICT Services; and • Core infrastructure is impacted and non-functional.	Activate ICT DRP.
Partial loss of a building.	Localised fire, explosion, bomb, sabotage, flooding, and power surge.	• Destruction of facilities and equipment in the affected area; • Possible damage to some areas of the building; and • Interruption of some business activities	Depending on the damage assessment report activate BCP/DRP as necessary
Denial of access to the building.	Public disturbances, civil unrest, closure by authorities, bomb threat.	• Staff cannot gain access to the building; • Limited, if any, impact on infrastructure; • Possible disruption of business activities; and • Critical systems can still be accessed remotely.	Access systems remotely; and perform business activities remotely for a limited time.

6. COMMUNICATION

The ICT Disaster Recovery Plan will be communicated to employees of the municipality so that it does not cause undue alarm to staff. The ICT Manager will explain that it is part of the planning that all businesses should undertake. The ICT Manager will ensure that the plan is updated regularly and that copies are readily available to all employees. Care will be taken to ensure that access to the contact details for staff is restricted to a smaller number of employees.

7. ICT DR TEAM

Swellendam Municipality will have a number of people that will be able to respond to an ICT disaster if it occurs. These people will be identified and trained in the disaster recovery processes.

Membership of these teams will be based on people's strengths and weaknesses and not only on the job that they do. This will be done to ensure that, in the event of an emergency; the people will not panic but will diligently follow the prepared plan. If a situation develops that is not in the ICT continuity plan, these people must be capable of reacting to the situation.

The persons that were identified are as follows:

a) Director Financial Services
b) ICT Steering Committee members,
c) ICT Manager,
d) ICT Recovery Administrator and his team (Service provider)
e) Disaster Manager

From the above ICT DR Team key members who carry the highest effort of responsibility and are ultimately responsible for all aspects of Disaster prevention and Disaster recovery, are:
a) ICT DR Team Leader; and
b) ICT Manager.

7.1 Crisis Control

In the context of Crisis Control, the ICT DR Team Leader and the ICT Manager with the recovery team shall:
a) Report to the Municipal Manager on the risks identified;
b) Provide a focal point for Swellendam Municipality to ensure the media and public receive the correct and non-contradictory information;
c) Ensure staff and relevant departments are made aware of the problems and the remedial action taken; and
d) Ensure that the Recovery Coordinator and Recovery Teams have the resources and support necessary to perform their duties.

7.2 Crisis Management

The team's core responsibility is to ensure that incidents that arise and escalations of incidents into crises or disasters are well managed and communicated in a manner that protects the organization's reputation.

Oversee the execution of the ICT Disaster Recovery Plan, Emergency Responses and Crisis Control.

7.3 Business Continuity Management

The main responsibility of the recovery team is to manage the response and recovery efforts until the resumption of normal business operations. These teams will operate at a tactical level and are comprised of Senior Management. In the event of a disaster, the team shall operate from a central point of command and be responsible for the following:

a) Invoking the relevant Disaster Recovery Plans and procedures.
b) Selecting an alternative central point of command when necessary;
c) Command and control all recovery processes and actions until the resumption of normal business operations;
d) Ensuring that recovery efforts are executed and will include the selection of alternative relocation options for staff, i.e. alternative off-site locations;
e) Updating the Municipal Manager on the progress of all business continuity and recovery efforts;
f) The Recovery teams shall also be responsible for the following pre-incident planning functions:
g) Ensuring that all applicable risk management policies, practices and procedures are enforced and complied with, to prevent the occurrence of disruptions and minimize their impact when they occur;
h) Ensuring the development, maintenance and testing of recovery plans addressing all "disaster" scenarios (including the maintenance of the overall ICT recovery program and its supporting infrastructure).

7.4 Damage Assessment

The responsibilities of the ICT Manager and his teams are to:

a) Evaluate the initial status of the damaged functional area and estimates both the time to reoccupy the facility and the recoverability of any remaining equipment;
b) It also has interfaces with affected external parties such as emergency service providers, and insurers.

8. CONTINGENCY STRATEGY

The contingency strategy aims to recover operations with minimal if any, impact on the services supplied to the Municipality customers. The contingency strategy focuses

on resolving issues relating to information technology, suppliers and services offered to Swellendam Municipality customers and, where appropriate the public.

Specifically, the contingency strategy focuses on:

a) Immediate welfare of staff employed at the service site
b) Assessing the workload requirements for Business Units
c) Establishing priorities for, and allocating the use of, technological and human resources
d) Delegating responsibilities for critical recovery procedures of each functional service area
e) Central control of recovering operations
f) Availability of data and relevant applications
g) Communicating the status of the event to the Municipal Manager.

9. INCIDENT MANAGEMENT

The configuration of Incident Management may vary with each emergency, depending on the type of specialist skills required. In the event of a disruption, whether from a predicted source or elsewhere, it will be activated.

The purpose of Incident Management is to determine whether the nature and extent of the disruption warrants deploying/activating the relevant ICT Disaster Recovery Plan and if so should:

a) Implement the selected procedures, securing the required resources where appropriate;
b) Identify, and where appropriate adapt, the relevant continuity procedures to ensure that the business continues to operate as near to normal manner as possible for the duration of the disruption;
c) Identify, and where appropriate adapt, the relevant recovery procedures to ensure that the business recovers from disruption in a timely and controlled manner once the root cause of the disruption has been eliminated;
d) Communicate with all parts of the organisation affected by the disruption on a regular basis regarding progress and the actions taken;
e) Organise, once recovery actions have been completed, a thorough review of its management of the disruption so all relevant lessons from the experience can be learned and incorporated into procedures and training programmes.

10. INFORMATION AND COMMUNICATION TECHNOLOGY RECOVERY TEAM (ICTRT)

The ICTRT will consist of senior representatives from the main business and support units. The ICTRT Leader will be the ICT Manager and will be responsible for taking overall

charge of the process and ensuring that the municipality returns to normal working operations as early as possible.

The purpose of the ICT Recovery Team is to determine the nature and extent of the disruption and should:

a) Co-ordinate the allocation of resources;
b) Co-ordinate the management of the undisrupted business;
c) Manage communication with Municipal Manager, associates and staff;

ICT recovery requires many types of resources. Those resources may include the following:

10.1 People

a) Recovery team members
b) Security guards
c) Cleaning staff
d) Drivers
e) Temporary employees
f) Supporting vendors

10.2 Supplies

a) Replacement office supplies
b) Recovery supplies
c) Computer printer paper, cartridges etc.
d) Health and Safety
e) Water
f) Sanitary

10.3 Equipment

a) Replacement production equipment
b) Additional production equipment
c) Replacement computer equipment
d) Additional computer equipment
e) Special recovery equipment
f) Furniture

11. INSURANCE

An important strategy to be considered is the maintenance of insurance to cover emergency losses, such as non-performance claims by clients, loss of income, or civil authority actions.

12. EMERGENCY RESTORATION SERVICES

Swellendam Municipality is allowed to procure goods and services under emergency per the procurement regulation without following the normal procurement process. The following are conditions under which the emergency procurement process may be utilised.

Emergency procurement is a procedure used by agencies to procure goods or services that are urgently needed and the procurement cannot be delayed by following the normal competitive procurement procedures.

Emergency procurements are authorized when:

a) There exists a threat to public health, welfare or safety.
b) Circumstances outside the control of the municipality and create an urgency of need, of which the delay does not permit the time involved in using more formal, competitive procedures.

The conditions warranting Emergency Procurement include the existence of one or more of the following:

a) The possibility of human injury or death,
b) The prevalence of human suffering or deprivation of rights,
c) The possibility of damage to property, or suffering and death of livestock and animals,
d) The interruption of essential services, including transportation and communication facilities or support services critical to the effective functioning of the Municipality as a whole,
e) The possibility of serious damage occurring to the natural environment,
f) The possibility that failure to take necessary action may result in the Municipality not being able to render an essential community service,
g) The prevailing situation, or imminent danger, should be of such a scale and nature that it could not readily be alleviated by interim measures, to allow time for the formal tender process.

Emergency Procurement must not be used in respect of the following:

a) To circumvent normal procurement procedures;
b) As a result of insufficient stock levels for items that are used daily.
c) As a result of working programs not properly planned;

The accounting officer must record the reasons for any deviations in terms of sub-regulation (1)(a) and (b) and report them to the next meeting of the council and include them as a note to the annual financial statements.

13. ICT SYSTEMS BACKUP AND RECOVERY STRATEGY

One of the most important aspects of ICT continuity planning is the choice of an appropriate strategy for the backup and recovery of ICT-based systems. Consideration should be given to the impact on the municipality's ICT systems of potential severe damage to premises or communications systems.

14. PREMISES AND ESSENTIAL EQUIPMENT BACKUP AND RECOVERY STRATEGY

Many unexpected events can affect premises and essential equipment vital to the continuation of normal business activities. This plan has therefore been developed to ensure continued service to customers in the event of a disaster affecting either the organisation's premises or its essential equipment.

The Municipality agreed on backup and recovery strategies for premises and essential equipment as follows:

Premises

Name of premises	Agreed backup and recovery strategy
Swellendam Municipality Head Office (IT services)	All personal computers will be configured in such a way that all important data is backed up centrally at the Head Office server room and alternative server room.

15. CUSTOMER SERVICE BACKUP AND RECOVERY STRATEGY

It is critical to be able to continue to provide an adequate level of service to the organisation's customers throughout an emergency, and this area has therefore been treated as a high priority when considering the preferred backup and recovery strategy.

16. INFORMATION AND DOCUMENTATION BACKUP AND RECOVERY STRATEGY

It is necessary to identify the dependencies that the organisation has on digitized information and to develop workable strategies for continuing an adequate level of business operations during a serious disruption, even though, in certain circumstances, access to such information may become difficult or even impossible.

17. REPLACEMENT PROCESS FOR FIREWALL

The firewall has an automatic failover in the event the firewall failed. The automatic switchover is managed by the IT Manager and IT Service Provider. Regular backups are made of the firewall.

18. SEPARATION DISTANCE

Alternative business sites to the server room will be the old server room in the Main Building. Backups are automatically synchronized every night to these sites from the Server room.

19. ICT DISASTER TEST PLAN

The ICT DR Plan must be periodically tested in a simulated environment to ensure that it can be implemented in emergencies and that the management and staff understand how it is to be executed.

Within any calendar year, the following test requirements are considered to be minimal:

a) Follow the Implementation Plan as provided in the ICT Test Plan;
b) At least one Simulation Lite test; and
c) At least one other test as defined in the Test Plan.

This part of the policy will only be implemented once a DR site has been established.

20. BACKUP SITE EQUIPMENT REQUIREMENTS

A backup site will later be established when enough funds are available at a location more than 6 kilometres away from the Municipal Main Offices with the necessary communication infrastructure and equipment to take over the complete functionality of the ICT systems in the case of a disaster, but only on a small scale until the Main site has been restored to its normal operations.

21. REVIEW

The ICT Disaster Recovery Policy must be approved by Council and be reviewed annually.

ICT FIREWALL RULES POLICY

1 July 2026

Table of Contents

1. PURPOSE OF THIS POLICY

This document serves to define the standard configuration of the main firewall separating the Municipality from the Internet.

2. GENERAL

The firewall must be a multi-homed firewall, with at least one physical network adapter per zone, or virtual adaptor in the case of virtualisation. Public zones not belonging to the Municipality (Internet, external providers, etc) may not be hosted on the internal zones. It must be separated from the internal zones by placing the public zones on a different network adapter.

3. FIREWALL ZONES

At least the following zones must be configured:

a) LAN: All subnets inside the Municipality.

b) WAN: The Internet.

c) DMZ: Isolated Zone hosting publicly accessible systems.

d) VPN: Users accessing the network via VPN services.

4. NETWORK ADDRESS TRANSLATION (NAT) POLICY

All traffic originating from the LAN zone, leaving the organisation must be masqueraded by applying source NAT and hiding the traffic behind the public IP address(es) used to exit the organization.

All traffic originating from the LAN zone, accessing services on the public-facing IP addresses in the DMZ must be masqueraded by applying source NAT and hiding the traffic behind the firewall's public IP address used to access that part of the DMZ.

All DMZ hosts must have public IP addresses or must be hidden behind one of the firewall's public IP addresses using destination NAT.

5. DEFAULT POLICIES

5.1 Global Default Policies

By default, all network traffic between all zones must be dropped without rejection notifications.

5.2 DMZ Default Policy

By default, no traffic is allowed from any host outside the DMZ zone to any host inside the DMZ zone other than the exceptions documented in this document.

By default, no traffic is allowed from any host in the DMZ zone to any host outside the DMZ zone other than the exceptions documented in this document.

5.3 Internet Default Policy

No host outside the organization (in the Internet zone) may communicate with any host inside the organization (in the DMZ or LAN zones) in any manner other than the exceptions documented in this document.

6. FIREWALL RULES

6.1 Incoming Services to LAN Hosts

a) Samras UAT Portal

The Samras UAT Portal gives the public access to their Municipal accounts. The web services on the Samras UAT Portal public IP address must be forwarded to the internal Samras UAT web server.

Source	Destination	Protocol(s)	Port	Action
WAN	Firewall - Samras UAT IP Address	TCP	443	Forward to Samras server

b) Reverse Web Proxy

The reverse web proxy must be hosted in the DMZ and access to http and https ports must be allowed in all zones.

Source	Destination	Protocol(s)	Port	Action	Comment
All zones	Reverse Proxy	TCP	80	Accept	HTTP
All zones	Reverse Proxy	TCP	443	Accept	HTTPS

Where possible external access to web services for any internal web server should be routed via the reverse web proxy. This adds an additional layer of security.

Further to this, internal http services should, where possible, be encrypted by the reverse web proxy and delivered to the public as https using a valid SSL certificate.

The following is a list of these web services:

Public Hostname	Action	Comment
intranet.swellendam.gov.za	Proxied to Zimbra Server	Zimbra E-mail and collaboration server.
intranet.swellendam.gov.za/hel pdesk	Proxied to the ICT helpdesk server	ICT Helpdesk and asset management system.
intranet.swellendam.gov.za/mu nlogos	Proxied to the local webserver on which the reverse proxy is hosted	Logo images and related files are used in e-mail signatures.

c) E-mail relay tunnel

Incoming e-mails and outgoing mail are relayed through an external server hosted in the cloud. This is to protect the public addresses of the Municipality from being blacklisted in the event of a security breach that results in unsolicited e-mail being sent from the local mail server. The mail server must have access to the cloud-hosted mail relay server in order to establish the tunnel.

Source	Destination	Protocol(s)	Port	Action	Comment
Local Mail server	Cloud relay server 0 relay03.wirelessweb.co.za	TCP	6595	Accept	Secure tunnelling port

6.2 Outgoing Access

Access to services hosted outside the organization must be filtered and controlled. This section defines the types of services that internal hosts are allowed to access on the Internet and additional controls that should be applied for each category of service.

a) Globally Allowed Outgoing Access

The following services are allowed between all computers in the organization and the Internet:

(i) SSH (TCP Port 22)

(ii) Ping (ICMP Port 8)

(iii) Traceroute (UDP Port 33434 to 33524 and ICMP Port 8)

b) Access to Internet websites

Internet websites should be categorized as best possible. Filtering policies must be defined which define the categories of websites that may be used and users must be connected to these policies.

Source	Destination	Protocol(s)	Port	Action	Comment
LAN	WAN	TCP	80	Allow, but apply filter policies	HTTP
LAN	WAN	TCP	443	Allow, but apply filter policies	HTTPS

c) Access to public NTP (Time) Servers

All local domain controllers should be able to update their time from any time server on the Internet.

Source	Destination	Protocol(s)	Port	Action	Comment
Domain Controllers	WAN	TCP/UDP	123	Allow	Time Services

d) Access to public DNS Servers

All local DNS servers should be able to query public DNS servers in order to serve name resolution queries to the local networks and to update their local DNS caches.

Source	Destination	Protocol(s)	Port	Action	Comment
Local DNS Servers	WAN	UDP	53	Allow	DNS

e) Sending and Receiving E-mail via External E-mail servers

The SAMRAS system sends accounts via an external SMTP server.

Source	Destination	Protocol(s)	Port	Action	Comment
SAMRAS	External E-mail Server Address	TCP	25	Allow	SMTP
SAMRAS	External E-mail Server Address	TCP	587	Allow	SMTP

f) Patch Management

The WSUS system requires internet access to download the latest patches.

Source	Destination	Protocol(s)	Port	Action	Comment
Security Server	Internet	TCP	80/443	Allow	HTTP and HTTPS

6.2 VPN Access

The following rules apply to VPN users dialled in via VPN:

a) Staff

Staff in the employ of the Municipality to whom VPN access has been granted must have full access to all resources in the LAN.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - Internal Users	LAN	All	All	Allow	
LAN	VPN - Internal Users	All	All	Allow	

b) ESRI Consultants

ESRI Consultants provide support on the GIS systems and may only have access to the internal GIS Servers.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - ESRI Consultants	GIS Servers	All	All	Allow	

c) Samras Consultants

Samras Consultants may only have access to the Samras servers.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - Samras Consultants	Samras Servers	All	All	Allow	

d) Collaborator Consultants

Collaborator Consultants may only have access to the Collaborator Servers.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - Collaborator Consultants	Collaborator Servers	All	All	Allow	

7. WEBSITE FILTERING POLICIES

7.1 Introduction

The default workspace policy will apply to all users by default. An approval process must be in place to allow users to request access to sites that are not allowed in the default policy.

7.2 Logging

All websites visited by all users must be logged.

7.3 Globally allowed websites

The following is a list of websites and website categories that everyone should have access to:

Site/Category	Description
Intranet Sites	All services provided by the organization to its employees.
Video Conferencing	Microsoft Teams and Zoom Video Conferencing.
Webmail	private email e.g. gmail.

7.4 Default Policy

By default access to all websites is granted except as defined below.

a) Default Policy - Blocked content

By default, the following categories of websites should be blocked:

Category	Description	Reason
Anonymizers	Sites offering Online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorized access	Security Risk and potentially allow users to circumvent company policies.
Criminal Activity	Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, burglary techniques and suicide	Illegal content.
Hacking	Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases.	Security Risk. Legal Risk.
Games	Sites providing information about or promoting electronic games, video games, computer games, role-playing games, or online games	Unproductive.
Nudity	Sites depicting nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect. It includes Nude images of film stars, models, nude art and photography	Inappropriate workplace conduct.
Peer-to-peer & torrents	Peer-to-Peer Activity	Primarily used for illegal downloads. Allow remote access to internal resources. Imposes legal and security risks. Negative impact on network bandwidth.

Category	Description	Reason
Personal Network Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.	Against policy.
Phishing and Fraud	Sites gathering personal information (such as name, address, credit card number, school, or personal schedules) that may be used for malicious intent	Security Threat.
Sexually Explicit	Adult sites not falling in "Porn, Nudity, Swimwear & Lingerie, Sex Education, and Sexual Health & Medicines" will be included in "Adult Content" and which may contain material not suitable to be viewed by audiences under 18	Inappropriate workplace conduct.
Social Networking	Dedicated Web sites to communicate informally with other members of the site, by posting messages, photographs, etc.	Unproductive.
Video Hosting	This category includes URLs that provide video searches.	Unproductive.
Video Streaming	Subscription Video Streaming	Unproductive.

7.5 Default Policy exceptions

The following policies are exceptions to the default policies. All the rules defined in the default policy will apply to users to whom these policies are applied, except for the exceptions defined below:

a) Media Access

This policy is designed for people in the organisation that require social media access to perform their duties.

Default Policy Exceptions
Social Networking

b) Social Media and Streaming Access

This policy is designed for people in the organisation that require social media access and access to media streaming to perform their duties.

Default Policy Exceptions
Social Networking
Video Hosting

c) Social Media and Cloud Storage

This policy is designed for people in the organisation that require social media access and access to cloud storage services to perform their duties.

Default Policy Exceptions
Social Networking
Personal Network Storage

d) Cloud Storage Access

This policy is designed for people in the organisation that require access to cloud storage services to perform their duties.

Default Policy Exceptions
Personal Network Storage

e) Streaming Access

This policy is designed for people in the organisation that require access to video streaming services to perform their duties.

Default Policy Exceptions
Video Hosting

7.6 Unrestricted Policy

This policy is designed for people in the organisation for whom no default policy applies. For this policy, everything is allowed, except for the following:

Blocked Categories
Criminal Activity

Nudity
Sexually Explicit

8 FIREWALL MANAGEMENT

The IT Department is responsible for implementing and maintaining Swellendam Municipality firewalls.

Swellendam Municipality has contracted with an IT service provider to manage the external firewalls. This service provider will be responsible for:

a) Configuration of firewalls
b) Firewall rule management
c) Retention of the firewall rules
d) Patch Management
e) Review the firewall logs for system errors
f) Blocked web sites
g) Attacks
h) Sending alerts to the IT Manager and CFO in the event of attacks or system errors
i) Backing up the firewalls

Firewall rule management is the process of periodically reviewing and optimizing firewall rules. This process involves the following:

a) Analyzing rule anomalies that affect the performance of the firewall.
b) Reordering existing rules to improve rule performance.
c) Identifying and removing unused rules.
d) Analyzing the impact of a new rule on the existing rule set before making it live in the firewall.
e) Recording the date the rule was added/change in a register.
f) Recording the name of the person who added/change the rule set.

Emergency Firewall Rule management changes must be submitted to the CFO for approval. Other Firewall Rule changes will be sent to the IT steering committee for consideration and update of the firewall rule policy.

9 SHORT TITLE

This policy is called the ICT Firewall Rules Policy of the Swellendam Municipality and will be reviewed annually.

ICT Governance Policy

1 July 2026

Table of Contents

1. ABBREVIATIONS

AG	Auditor-General of South Africa
CMMI	Capability Maturity Model Integration
CIO	Chief Information Officer
CGICTPF	Corporate Governance of ICT Policy Framework
COBIT®	Control Objectives for Information Technology
DPSA	Department of Public Service and Administration
DCOG	Department of Cooperative Governance
ICT	Information and Communications Technology
ISACA®	Information Systems Audit and Control Association
ISO/IEC	International Organisation for Standardisation (ISO) and the International Electro-Technical Commission (IEC)
ISO/IEC 38500	International Standard on Corporate Governance of ICT (ISO/IEC WD 38500: 2008: 1)
ITGI™	ICT Governance Institute
ITIL	The Information Technology Infrastructure Library
King III	The King III Report and Code on Governance for South Africa
MICTGPF	Municipal ICT Governance Policy Framework
M&E	Monitoring and Evaluation
PSCGICTPF	Public Service Corporate ICT Governance Policy Framework
SALGA	South African Local Government Association
SDBIP	Service Delivery and Budget Implementation Plan

2. ICT GOVERNANCE OVERVIEW

2.1 Information and Communications Technology (ICT) Governance has been described as the effective and efficient management of ICT resources to facilitate the achievement of organizational goals and objectives. ICT does not exist for its own sake within an organisation, ICT is there to make sure that organizations achieve sustainable success through the use of their ICT.

2.2 The ICT Governance Institute describes ICT Governance as, "...the responsibility of the board of directors and executive management. ICT is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's ICT [the infrastructure as well as the capabilities and organisation that is established to support ICT] sustain and extends the organisation's strategies and objectives".

2.3 Governance has risen in importance because of the widening gulf between what the organization expects and what ICT delivers. ICT has grown to be seen as a cost centre with growing benefits to the organisation ICT serves. An ICT Governance framework is meant to align ICT functions to the organizational goals, minimise the risk ICT introduces and ensure that there is value in the investment made in ICT.

2.4 The view that ICT should be governed and managed at all levels within a given organizational structure is supported by internationally accepted good practices and standards. These practices and standards are defined in the King III Code of Good Governance, ISO 38500 Standard for the Corporate Governance of ICT and other best practice ICT Process Frameworks which form the basis of this document.

2.5 Translated into a municipal operating environment the corporate governance of ICT places a very specific responsibility on the Council and Management within a municipality to ensure that the decision-making process for ICT-related investments and the operational efficiencies of the municipality's ICT environments remain transparent and are upheld. This accountability enables the municipality to align the delivery of ICT services with the municipality's Integrated Development Plans and strategic goals.

2.6 The Council and Management of municipalities need to extend their governance functions to include the Corporate Governance of ICT. In the execution of the Corporate Governance of ICT, they should provide the necessary strategies, architectures, plans, frameworks, policies, structures, procedures, processes, mechanisms and controls, and culture which comply with the best practice of ICT Governance Frameworks.

2.7 To strengthen the Corporate Governance of ICT further, responsibility for the decision-making of ICT programmes and projects should be placed at a strategic level in the municipality. The Corporate Governance of ICT is a continuous function that should be embedded in all operations of a municipality, from the Council and Management level to all areas within a municipality including ICT service delivery.

2.8 According to the established frameworks, the Governance of ICT is implemented in two different layers:

2.8.1 Corporate Governance of ICT – the Governance of ICT through structures, policies and processes, in other words, the system by which the current and future use of ICT is directed and controlled.

2.8.2 Governance of ICT – through Standard Operating Procedures, in other words, the individual processes and procedures which ensure the

compliance of the ICT environment based on a pre-agreed set of principles.

2.9 To address the above-mentioned, the Western Cape Department of Local Government in collaboration with the Department of Cooperative Governance (DCOG), the Department of Public Service and Administration (DPSA), the South African Local Government Association (SALGA), and the Western Cape Provincial Treasury, developed this Municipal Corporate Governance of ICT Policy for application in the Local Government sphere.

2.10 The purpose of the Municipal ICT Governance Policy is to institutionalise the Governance of ICT as an integral part of corporate governance within municipalities. This Municipal ICT Governance Policy Framework provides the Municipal Council and Management within a municipality with a set of principles and practices that must be complied with, together with an implementation approach to be utilised for the implementation of ICT Governance within Municipalities.

2.11 To enable a municipality to implement this Municipal Corporate Governance of ICT Policy, a three-phase approach will be followed:

2.11.1 Phase 1 – Enabling Environment: The Corporate Governance of ICT environments will be established in Municipalities through the adoption of this Municipal Corporate Governance of ICT Policy and its associated policies through Council resolution;

2.11.2 Phase 2 – Business and Strategic Alignment: Municipalities will plan and implement the alignment between IDP's, strategic goals and ICT strategy.

2.11.3 Phase 3 – Continuous Improvement: Municipalities will enter into an ongoing process to achieve continuous improvement of all elements related to the Governance of ICT.

2.12 This Corporate Governance of ICT Policy will allow municipalities to maintain alignment of strategic ICT functions to meet their needs and apply best practices to reduce costs and increase the effectiveness of the ICT service delivery to the municipality.

3. PURPOSE

3.1 The purpose of this policy is to institutionalise the Corporate Governance of ICT as an integral part of corporate governance within municipalities in a uniform and coordinated manner. The policy provides a set of principles and practices which will assist to institutionalise the Corporate Governance of ICT.

4. LEGISLATIVE FRAMEWORK

4.1 The following legislation, among others, was considered in the drafting of this policy/plan:

4.1.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
4.1.2 Copyright Act, Act No. 98 of 1978;
4.1.3 Electronic Communications and Transactions Act, Act No. 25 of 2002;
4.1.4 Minimum Information Security Standards, as approved by Cabinet in 1996;
4.1.5 Municipal Finance Management Act, Act No. 56 of 2003;
4.1.6 Municipal Structures Act, Act No. 117 of 1998;
4.1.7 Municipal Systems Act, Act No. 32, of 2000;
4.1.8 National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
4.1.9 Promotion of Access to Information Act, Act No. 2 of 2000;

4.1.10 Protection of Personal Information Act, Act No. 4 of 2013;

4.1.11 The Disaster Management Act, Act No. 57 of 2002; Regulation of Interception of Communications Act, Act No. 70 of 2002; and

4.1.12 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

5. BENEFITS OF GOOD GOVERNANCE OF ICT

5.1 When the Governance of ICT is effectively implemented and maintained, the following benefits are realised:

5.1.1 Establishment of ICT as a strategic enabler in a municipality.

5.1.2 Improved achievement of municipal integrated development plans;

5.1.3 Improved effective service delivery through ICT-enabled access to municipal information and services;

5.1.4 Improved ICT enablement of a municipality;

5.1.5 Improved delivery of ICT service quality;

5.1.6 Improved stakeholder communication;

5.1.7 Improved trust between the municipality and the community through the use of ICT

5.1.8 Lower costs (for ICT functions and ICT-dependent functions)

5.1.9 Increased alignment of ICT investment towards municipal integrated development plans;

(i) Improved return on ICT investments;

(ii) ICT risks are managed in line with the ICT priorities and risk appetite of the municipality

(iii) Appropriate security measures to protect both the municipality's and its employee's information;

(iv) Improved management of municipal-related ICT projects;

(v) Improved management of information as ICT is prioritised on the same level as other resources in municipalities;

(vi) ICT pro-actively recognises potential efficiencies and guides municipalities in timeous adoption of appropriate technology;

(vii) Improved ICT ability and agility to adapt to changing circumstances; and

(viii) ICT is executed in line with legislative and regulatory requirements.

6. CORPORATE GOVERNANCE OF ICT GOOD PRACTICE AND STANDARDS

6.1 In recognition of the importance of ICT Governance, a number of internationally recognised frameworks and standards, have been developed to provide context for the institutionalisation of the governance of ICT:

6.1.1 The **King IV Code:** The most commonly accepted Corporate Governance Framework in South Africa is also valid for Municipalities. ICT was used to inform the Governance of ICT principles and practices and to establish the relationship between Corporate Governance of and Governance of ICT.

6.1.2 **ISO/IEC 38500:** Internationally accepted as the standard for Corporate Governance of ICT; ICT provides governance principles and a model for the effective, efficient, and acceptable use of ICT within municipalities.

6.1.3 **Other** internationally accepted process frameworks for implementing Governance of ICT.

7. LAYERED APPROACH TO CORPORATE GOVERNANCE OF ICT IN MUNICIPALITIES

7.1 Corporate Governance of ICT encompasses two levels of decision-making, authority and accountability to satisfy the expectations of all stakeholders. These levels are:

7.1.1 Facilitating the achievement of a municipality's strategic goals (Corporate Governance of ICT); and

7.1.2 The efficient and effective management of ICT service delivery (Operational Governance of ICT).

7.2 The implementation of Corporate Governance of ICT in Municipalities thus consists of the following layered approach:

7.2.1 This Municipal Corporate Governance of ICT Policy addresses the Corporate Governance of the ICT layer.

7.2.2 Other best practice frameworks will be adapted to give effect to the governance of the ICT operational environments within municipalities.

8. CORPORATE GOVERNANCE IN MUNICIPALITIES:

8.1 Corporate governance is a vehicle through which value is created within a municipal context. Value creation means realising benefits while optimising resources and risks. This value creation takes place within a governance system that is established by the municipal policy framework. A governance system refers to all the means and mechanisms that enable the municipality's Council and Management team to have a structured and organised process.

8.2 The Corporate Governance of ICT is an integral part of the governance system in municipalities. The Corporate Governance of ICT involves evaluating, directing and monitoring the alignment of the municipal ICT strategy with the municipal IDP's and related strategies. The Corporate Governance of ICT also involves the monitoring of ICT service delivery to ensure a culture of continuous ICT service improvements exists in the municipality.

8.3 The Corporate Governance of ICT includes determining ICT strategic goals and plans for ICT service delivery as determined by the Service Delivery and Budget Implementation Plan (SDBIP) objectives of the municipality.

9. MUNICIPAL CORPORATE GOVERNANCE OF ICT POLICY OBJECTIVES

9.1 The objectives of this Corporate Governance of ICT Policy for municipalities seek to achieve the following:

9.1.1 Institutionalising a Corporate Governance of ICT Policy that is consistent with the Corporate Governance Frameworks of the municipality;

9.1.2 Aligning the ICT strategic goals and objectives with the municipality's strategic goals and objectives;

9.1.3 Ensuring that optimum Municipal value is realised from ICT-related investment, services and assets;

9.1.4 Ensuring that Municipal and ICT-related risks do not exceed the municipality's risk appetite and risk tolerance;

9.1.5 Ensuring that ICT-related resource needs are met optimally by providing the organisational structure, capacity and capability;

9.1.6 Ensuring that the communication with stakeholders is transparent, relevant and timely; and

9.1.7 Ensuring transparency of performance and conformance and driving the achievement of strategic goals through monitoring and evaluation.

10. PRINCIPLES FOR THE CORPORATE GOVERNANCE OF ICT IN MUNICIPALITIES:

10.1 This Municipal Corporate Governance of ICT Policy is based on principles as explained in international good practices and standards for ICT governance, namely, King III Code, ISO/IEC 38500 and other best practice process frameworks.

10.2 The principles which have been adopted in the Public Service Corporate ICT Governance Policy Framework (PSCGICTPF) which have been adapted for municipalities.

10.2.1 Principle 1: Political Mandate

The Governance of ICT must enable the municipality's political mandate. The Municipal Council must ensure that the Corporate Governance of ICT achieves the service delivery mandate of the municipality.

10.2.2 Principle 2: Strategic Mandate

The Governance of ICT must enable the municipality's strategic mandate. The Municipal Manager must ensure that Corporate Governance of ICT serves as an enabler of the municipality's strategic plans.

10.2.3Principle 3: Corporate Governance of ICT

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 legislative and regulatory landscape and information security context.

10.2.4 Principle 4: ICT Strategic Alignment

ICT service delivery must be aligned with the strategic goals of the municipality. Management must ensure that ICT service delivery is aligned with the municipal strategic goals and that the administration accounts for the current and future capabilities of ICT. ICT must ensure that ICT is fit for purpose at the correct service levels and quality for both current and future Municipal needs is met.

10.2.5 Principle 5: Significant ICT Expenditure

Management must monitor and evaluate significant ICT expenditures. Management must monitor and evaluate major ICT expenditures, ensure that ICT expenditure is made for valid Municipal enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure while ensuring that information assets are adequately managed.

10.2.6 Principle 6: Risk Management and Assurance

Management must ensure that ICT risks are managed and that the ICT function is audited. Management must ensure that ICT risks are managed within the municipal risk management practice. ICT must also ensure that the ICT function is audited as part of the municipal audit plan.

10.2.7 Principle 7: Organisational Behaviour

Management must ensure that ICT service delivery is sensitive to organisational behaviour/culture. Management must ensure that the use of ICT demonstrates an understanding of and respect for organisational behaviour/culture.

11. MUNICIPAL CORPORATE GOVERNANCE of ICT POLICY

11.1 The following functions have been assigned to specific designated municipal structures and officials to achieve the objectives and principles contained in this Municipal Corporate Governance of ICT Policy:

11.2 The Municipal Council must:

11.2.1 Provide political leadership and strategic direction through, approving ICT Policy and providing oversight;

11.2.2 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;

11.2.3 Assist the Municipal Manager to deal with intergovernmental, political and other ICT-related municipal issues beyond their direct control and influence; and Ensure that the municipality's organisational structure makes provision for the Corporate Governance of ICT.

11.3 The Municipal Manager must:

11.3.1 Provide strategic leadership and management of ICT,

11.3.2 Ensure alignment of the ICT strategic plan with the municipal IDP;

11.3.3 Ensure that the Corporate Governance of ICT is placed on the municipality's strategic agenda;

11.3.4 Ensure that the Corporate Governance of the ICT Policy Framework, charter and related policies for the institutionalisation of the Corporate Governance of ICT are developed and implemented by management;

11.3.5 Determine the delegation of authority, personal responsibilities and accountability to the Management with regard to the Corporate Governance of ICT;

11.3.6 Ensure the realisation of municipality-wide value through ICT service delivery and management of Municipal and ICT-related risks;

11.3.7 Ensure that appropriate ICT capability and capacity are provided and a suitably qualified and experienced Governance Champion is designated.

11.3.8 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.

11.3.9 Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of the ICT system e.g. ICT steering committee.

11.4 The Municipal ICT Steering Committee, Risk and Audit Committee must:

11.4.1 Assist the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.

11.5 Management must ensure:

11.5.1 ICT strategic goals are aligned with the municipality's Municipal strategic goals and support;

11.5.2 The Municipal-related ICT strategic goals are cascaded throughout the municipality for implementation and are reported on.

12. PRACTICAL IMPLEMENTATION OF THIS ICT GOVERNANCE POLICY.

12.1 Upon approval of this Policy, the municipality must approve a Corporate Governance of ICT Charter and practical implementation plan.

12.2 The Charter should guide the creation and maintenance of effective enabling governance structures, processes and practices. ICT should also clarify the governance of ICT-related roles and responsibilities towards achieving the municipality's strategic goals.

12.3 In order to give effect to the Corporate Governance of ICT in Municipalities, the following objectives should be included in the municipality's ICT Governance charter:

12.3.1 Identify and establish a Corporate Governance of ICT Policy and implementation guidelines for the municipality;

12.3.2 Embed the Corporate Governance of ICT as a subset of the municipal governance objectives.

12.3.3 Create Municipal value through ICT enablement by ensuring municipal IDP and ICT strategic alignment;

12.3.4 Provide relevant ICT resources, organisational structure, capacity and capability to enable ICT service delivery;

12.3.5 Achieve and monitor ICT service delivery performance and conformance to relevant internal and external policies, frameworks, laws, regulations, standards and practices;

12.3.6 Implement the governance of ICT in the municipality, based on an approved implementation plan.

13. DESIGN OF THE MUNICIPAL CORPORATE GOVERNANCE of ICT CHARTER

13.1 This charter should be approved at a strategic level in the municipality and should contain the following:

13.1.1 How the ICT strategic goals and their related service delivery mechanisms will be aligned with municipal IDP, monitored and reported on to the relevant stakeholders;

13.1.2 How ICT service delivery will be guided at a strategic level to create ICT value in the municipality;

13.1.3 How the administration ICT-related risks will be managed;

13.1.4 The establishment of structures to give effect to the Governance of ICT, and the management of ICT functions. The members of these structures and the roles, responsibilities and delegations of each should be defined.

13.2 The proposed structures are as follows:

13.2.1 ICT STEERING COMMITTEE (Committee of Management)

13.2.2 The members of the ICT Steering are as follows:

(i) Designated Members of Management and the ICT Manager.

(ii) The Chairperson shall be a designated member of the Management of the Municipality duly appointed by the Municipal Manager.

13.2.3 The mandate/responsibilities are:

(i) Has a specific delegated responsibility to ensure the planning, monitoring and evaluation, of the municipalities ICT structures and ICT policies.

(ii) Planning and monitoring of the ICT procedures, processes, mechanisms and controls regarding all aspects of ICT use (Municipal and ICT) are clearly defined, implemented and enforced

(iii) ICT Performance Management.

(iv) ICT Change Management.

(v) ICT Contingency Plans.

(vi) ICT Strategy Development.

(vii) Management of ICT Security and Data Integrity.

(viii) The establishment of the municipalities ICT Ethical culture.

(ix) The evaluation, directing and monitoring of ICT-specific projects.

(x) ICT Strategic Alignment.

(xi) ICT Governance Compliance.

(xii) ICT Infrastructure Management.

(xiii) ICT Security.

(xiv) ICT Application Management.

(xv) ICT Value.

(xvi) ICT Data availability and integrity.

(xvii) ICT Vendor Management.

(xviii) The evaluation, directing and monitoring of ICT processes

13.2.4 Audit Committee and Risk Committee

13.2.5 The members of the Audit Committee and Risk Committee are as follows:

(i) Nominated members of the Audit and Risk committee/s of the municipality;

(ii) The CFO or ICT Manager.

13.2.6 The mandate/responsibilities are:

(i) Has a specific responsibility to perform an oversight role for the Identification and Management of ICT audit and governance compliance, and ICT Risks.

14. MUNICIPAL IDP AND ICT STRATEGIC ALIGNMENT

14.1 This accountability assigned to the leadership of a municipality through this ICT Corporate Governance Policy Framework enables the municipality to align the delivery of ICT strategies and services with the municipality's Integrated Development Plans and strategic goals.

14.2 This is achieved through the development and adoption of an ICT strategic plan which is informed by the enterprise architecture plan which clearly outlined the roles, responsibilities and business processes contained in the IDP.

15. CONTINUOUS SERVICE IMPROVEMENT OF ICT IN MUNICIPALITIES

15.1 In this phase, detailed measurable criteria for the implementation of and compliance against the approved ICT Corporate Governance Policy and implementation plan are established and can be measured for compliance.

15.2 In this phase, the applicability of all elements of the ICT Corporate Governance Policy Framework is tested for efficacy and efficiency.

16. THE DETAILED PHASED APPROACH

16.1 Implementation deliverables per financial year

16.1.1 **Phase 1 (Enablement Phase):** Completed by June 2017 (Finalised)

(i) Municipal Corporate Governance of ICT Policy approved and implemented;
(ii) ICT Governance Charter approved and implemented;
(iii) Governance Champion designated and responsibilities allocated;
(iv) A proficient ICT Manager or CIO appointed functioning at a strategic level.
(v) Approved and implemented ICT Governance Framework;
(vi) Approved ICT Disaster Recovery Plan informed by Municipal Continuity Plan and Strategy.
(vii) Approved ICT User Access Management policy.
(viii) Approved **ICT Security Controls policy.**

16.1.2 Phase 2 (Strategic Alignment): Completed by June 2019

(i) Approved ICT Strategic Plan;
(ii) Approved ICT Performance Indicators as contained in the municipality's performance management system.

16.1.3 Phase 3: Continuous improvement of Corporate Governance and Governance of ICT

(i) The successful implementation of a Corporate Governance of the ICT system leads to continuous improvement in the creation of value for the municipality. ICT delivery must be assessed on an ongoing basis to identify gaps between what was expected and what was realised. Assessments must be performed coherently and encompass both the Corporate Governance of ICT (ICT contribution

to the realisation of Municipal value) and the Governance of ICT. (Continuous improvement of the management of ICT)

17. CONCLUSION

17.1 This Corporate Governance of ICT Policy has been designed for the exclusive use and alignment of Municipalities. The Implementation thereof had been phased over a longer period to provide municipalities with the time required to implement this ICT Governance Policy Framework effectively.

17.2 The policy will be reviewed annually.

ICT USER AND NETWORK ACCESS POLICY

1 July 2026

Table of Contents

1. ABBREVIATIONS

"ICT" refers to Information Communication Technology.

"IT" refers to Information Technology.

"SWDM" refers to Swellendam Municipality.

"*Municipality"* refers to the Swellendam Municipality.

"email" refers to electronic mail

"MM" refers to the Municipal Manager.

"Site Manager" refers to the service provider appointed to provide technical support.

"Manager ICT Services" refers to the Head of the ICT Services Division

"CFO" refers to the Chief Financial Officer.

"SAPS" refers to the South African Police Services

"SCM" refers to Supply Chain Management

"HR" refers to Human Resource Management

"Users" refers to Councillors, Employees, End Users, Interns, Temporary Staff Members and Contract Workers

"Manager" refers to the Head of each Division

"Network Devices" refers to computers and devices interconnected by communications channels that facilitate communications among users.

"IR" refers to the Information Resources.

"SLA" refers to Service Level Agreement.

"Workstations" refers to computers, laptops, printers and photocopiers

"VPN" refers to Virtual Private Network

"ISO" refers to International Organization for Standardization

"POPIA" refers to the Protection of Personal Information Act

2. PREAMBLE

2.1 SWDM ICT Division has developed the SWDM ICT User and Network Access Policy to establish specific requirements for accessing SWDM IR and monitoring.

2.2 SWDM ICT User and Network Access Policy protect SWDM IR from accidental and/or negligent deletion, destruction and modification.

2.3 Formal procedures must be put in place:

2.3.1 that will control who will have access to what type of information,

2.3.2 determine the privilege levels that each information user will have.

2.3.3 control how access is granted and how such access is changed and the period of such access.

2.4 The policy also mandates a standard for the creation of strong passwords, password protection and frequency of changing passwords. Modification and/or destruction of information should be traced.

3. USER AWARENESS

3.1 Every councillor, employee, contractor and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when using the Municipality's computers, networks, data and other information resources. Each user is responsible for reporting any suspected breaches of this policy's terms to the Manager: ICT Services.

3.2 The contents of this policy will be made available through presentations to all staff members and all those who attend must sign an attendance register and/or email and/or place it on the SWDM Network.

4. PURPOSE

4.1 The purpose of this policy is to protect and monitor the Municipality's ICT resources and to safeguard the confidentiality and integrity of information, resources, data, ICT equipment and council documentation.

4.2 This policy will guide the controls to be put in place:

- 4.2.1 By controlling who has the right to use what type of information,
- 4.2.2 Monitoring the network,
- 4.2.3 Generating stability and vulnerability reports,
- 4.2.4 and guard against unauthorized use and access to information.

5. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY

5.1 COBIT 5
5.2 ISO/IEC 20000
5.3 ISO/IEC 27000
5.4 ITIL v3
5.5 SWDM ICT Security and Firewall Policy
5.6 Information Technology Standard Operating procedures (To be developed)

6. ROLES AND RESPONSIBILITIES

6.1 This policy applies to every network user of SWDM including and not limited to councillors, staff members, third-party service providers, partners, interns, contract workers, services and agents:

- 6.1.1 SWDM ICT Division is responsible for ensuring that IR is maintained in compliance with the Municipality's ICT User and Network Access policy and procedures.

6.1.2 The Manager of the ICT Services Division is responsible for monitoring compliance with the Municipality's ICT User and Network Access Policy.

6.1.3 All SWDM ICT Service Division Team members are responsible to make sure that they adhere to the SWDM ICT User and Network Access Policy and that they enforce this policy.

6.1.4 HR must alert SWDM the Manager of the ICT Services Division of new network access needs whenever new appointments are made and inform when employees terminate their services.

6.1.5 The Manager of the ICT Services Division shall inform the Help Desk of any terminations of services so that the user names are disabled.

6.1.6 It is the user's responsibility to ensure that they safeguard their passwords to prevent being used to gain unauthorized access to the network. It is the user's responsibility to ensure that they do not leave their computers active while not attending and ensure that it is either lock it or log off.

7. ENFORCEMENT/LEGAL FRAMEWORK

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

7.2. Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations and policy prescripts (this list is by no means exhaustive):

7.2.1. Amended State Information Technology Agency Act, 2002

7.2.2. Promotion of Access to Information Act, 2000

7.2.3. Municipal Finance Management Act, 2003

7.2.4. Municipal Systems Act, 2000

7.2.5. Copyright Act, 1978

7.2.6. National Archives Act, 2003

7.2.7. Protection of Personal Information Act, 2013

7.2.8. King Code of Government Principles (King IV)

7.2.9. Electronic Communication and Transaction Act, 2002

7.2.10. Any other applicable legislation, regulation or policy.

8. USER AND NETWORK ACCESS POLICY

8.1 Formal user access control must be documented, implemented and kept up to date for application and information systems to ensure authorized user access and prevent unauthorized user access.

8.2 The process and physical access must be documented from the moment the user is registered on the network until the time the user is deregistered on the network.

8.3 Each user must be granted access and rights according to their needs and job.

8.4 Each user's access rights must be reviewed yearly by the Manager of ICT Services.

8.5 Only SWDM ICT Service Division officials must have administrative rights and they must be recorded as such. Any other person that needs to have administrative rights will be recorded and the rights will be removed at the end of the session.

8.6 All third-party vendor physical access to the server and switch room must be logged in a register in the format (Name, Surname, Company, Purpose, Date and Time) and must be accompanied by an SWDM ICT Service Division official at all times.

8.7 Third-party service providers will only be granted controlled access to remotely access the network by Director: ICT Services under strict supervision by SWDM ICT Services Division official or its appointed party. Audit trails must be in place at all times. The Service Provider must provide access to audit trail reports.

8.8 All user access forms shall be signed off by the ICT Manager and Director Financial Services and filed for safekeeping.

9. USER ACCOUNT MANAGEMENT

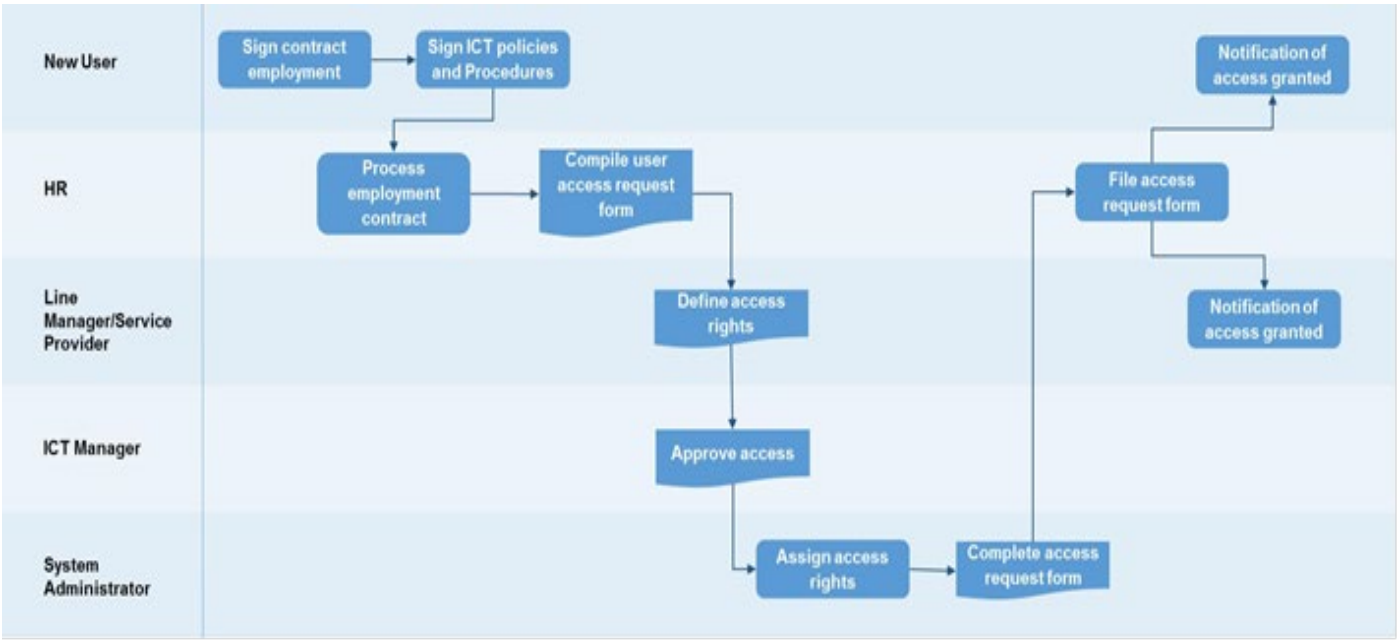
9.1 *New User Registration*

9.1.1 Each employee that requires access to the SWDM network shall complete the network access form which is provided by the ICT Manager and must be recommended by the Director of the employee for registration of the user account.

9.1.2 Network access forms must be approved by the Manager of ICT Services and Director Financial Services.

9.1.3 No network access shall be granted to unauthenticated individuals.

9.1.4 The following diagram below indicates the formal new user registration process:



9.2 *Termination of Users*

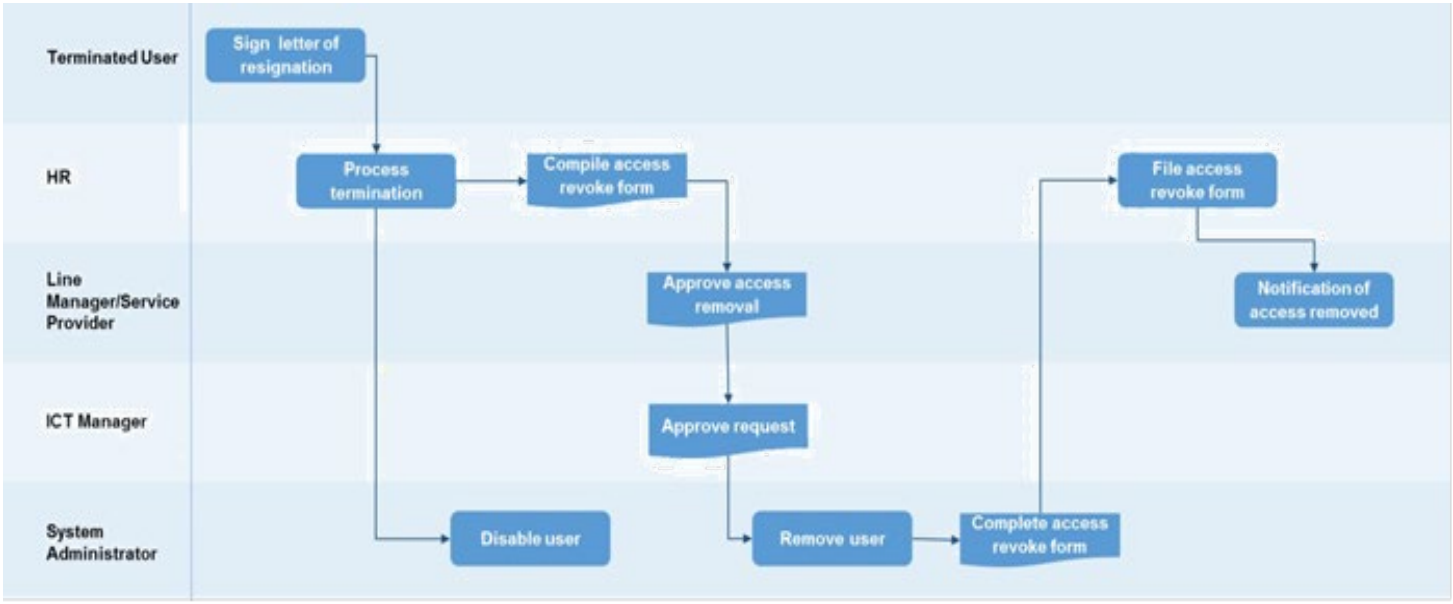
9.2.1 When the employee ceases to work for SWDM it is the responsibility of HR to inform the ICT Service Division of such termination of employment.

9.2.2 The ICT Service Division will disable the account of such users within three (3) days of receipt of the termination form. ICT Services Division shall effect such termination on Active Directory, Exchange Server and any other network services.

9.2.3 The ICT Service Division shall not terminate any user account without being informed by HR or the relevant Director of such need to terminate.

9.2.4 All user accounts and mailboxes may be deleted immediately by the ICT Services Division, upon an employee's departure from the Municipality either by dismissal, transfer, resignation, retirement, death or any other form of departure as informed by HR.

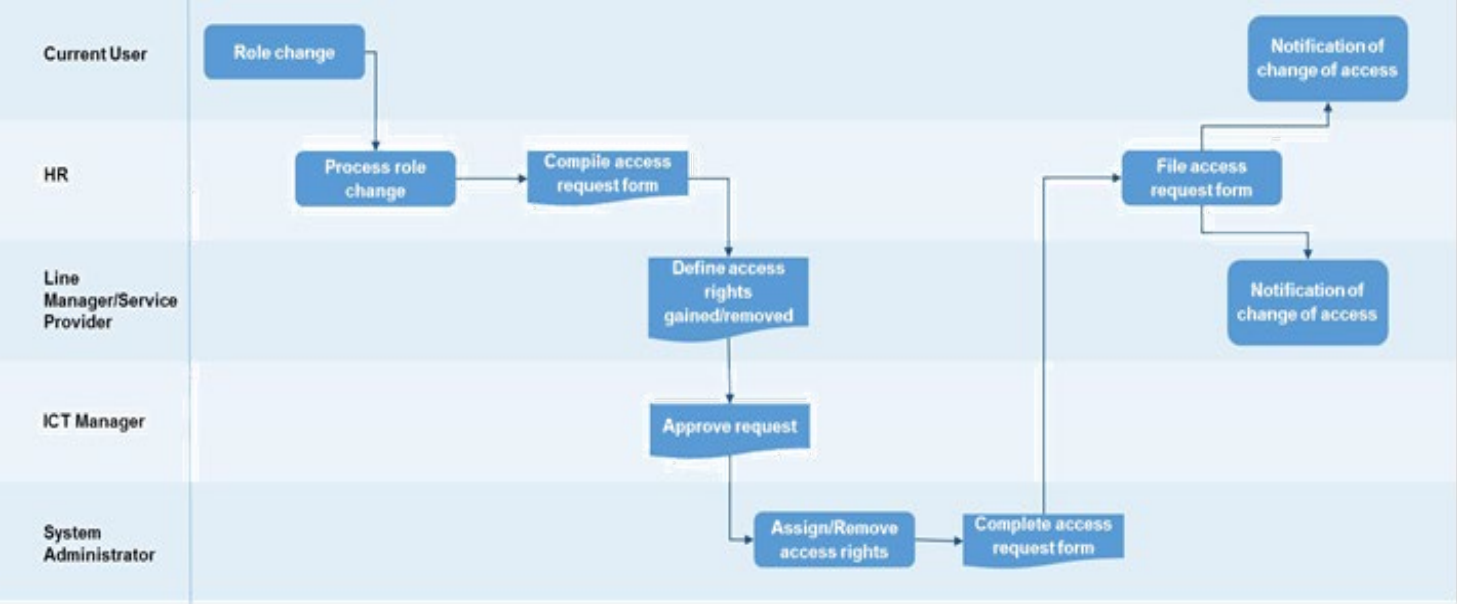
9.2.5 The following diagram below indicates the formal new user termination process:



9.3 *User Access Change Request*

9.3.1 An employee's access to a user account will be changed/modified by ICT Services Division, once the employee has transferred to a different Division per the employee's new job functions and requirements as recommended by the relevant Director

9.3.2 No user account will be created or modified without a signed network access form by the relevant Director and approved by the Director of Financial Services.



9.4 *General User Access Rights Management*

9.4.1 There shall be a register maintained by the ICT Manager to record terminations and new appointments and such information will form part of the ICT Service Division monthly reports and be reported to the ICT Steercom meetings quarterly.

9.4.2 All user accounts at the Municipality are created as Standard User Accounts. This means that users have standard privileges to log onto the network, use network printers that have been assigned to them,

access their email, and use the internet and any other privilege that is a core requirement of their job function.

9.4.3 Access rights may include, but are not limited to:

a) General office applications (E-mail, Microsoft Office, SharePoint, etc.);
b) Department-specific applications and/or databases;
c) Network Shares;
d) Administrative tasks;
e) RAS/VPN Access;
f) Wi-Fi; and
g) BYOD – Bring Your Own Device

9.4.4 Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.

9.4.5 RAS/VPN access must only be granted to users who require the service to fulfil their business functions.

9.4.6 RAS access must only be granted to employees who require remote access to a system to administer the environment.

9.4.7 VPN access must only be granted to employees who:

(a) Work remotely (Not at the office);
(b) Work overtime, or not within regular office hours.

9.4.8 It is the responsibility of the ICT Manager to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.

9.4.9 RAS/VPN access must be monitored and audit logs reviewed every quarter (3 months) by system administrators.

9.4.10 All reviews must be formally documented and signed off by the ICT Manager and Director of Financial Services.

9.4.11 Documentation must be kept for record-keeping purposes.

9.4.12 The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors if it is to be used for official purposes (BYOD).

9.4.13 The ICT team must ensure that all mobile devices must be protected with a PIN.

9.5 User Accounts

9.5.1 User names are standardized and the employee's name and the first letter of the surname are used to enable the user to log onto the network and the user's computer.

9.5.2 All dormant user accounts will be deleted or disabled thirty (30) days after the user has been informed that their account has not been used for longer than thirty (30) days. If the user cannot be contacted the supervisor shall be informed accordingly.

9.5.3 Should it be discovered that the user has not been able to access the computer account due to leave, the account shall be disabled.

9.5.4 Should it be discovered that an account has not been accessed or be used for a period of hundred and twenty (120) consecutive days such an account shall be deleted without notice.

9.5.5 Email addresses are also standardized with the employee's name and the first letter of the user's surname. In the instance where there are users with the same name and first letter of the user's surname, the user's full name and another initial and surname may be used as an email address.

10. PASSWORD MANAGEMENT

10.1 The password that an employee uses to log onto the network will be applied to access the employee's email account and internet application.

10.2 The Mayor, the Speaker, the Chief Whip, full-time and part-time Councillors, Interns and temporarily appointed contractors will be issued with usernames and passwords, which will be operative until their service is terminated.

10.3 Passwords must not contain the user's entire parts of the user's Surname or Name.

10.4 Passwords must contain characters from three of the following five categories:

- 10.4.1 Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- 10.4.2 Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)
- 10.4.3 Base 10 digits (0 through 9)
- 10.4.4 Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- 10.4.5 Non alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/

10.5 Passwords must never be written down on a piece of paper or shared with anyone. Passwords must be kept safe and secret.

10.6 Use different passwords for all user accounts.

10.7 Passwords should be changed every 30 days.

10.8 No official is allowed to show or share their passwords with any work colleague or the ICT Service Division for any reason.

11. OPERATING SYSTEM ACCESS RIGHTS

11.1 Each system administrator must be given their own account within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the ICT Steering Committee.

11.2 The default administrator account must be renamed and a password must be randomly generated and sealed in an envelope and kept in a safe.

11.3 The default guest account must be removed or renamed and disabled.

11.4 Segregation of duties must be practised, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.

11.5 Applications administrators must remain independent of the department utilising the application, except for the ICT Services Division.

11.6 The ICT Manager must review monthly all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

11.7 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record-keeping purposes.

12. REMOTE ACCESS CONNECTIONS

12.1 A remote access connection is only allowed for server access and authorization must be granted by the Manager: ICT Services and Director Financial Services.

12.2 An application form must be completed by the third party required access to the SWDM network.

12.3 The ICT Manager will be responsible to maintain a register of all remote access granted.

12.4 All activities must be monitored monthly by the ICT Manager and changes should be recorded in the register accordingly.

13. SERVER ACCESS

13.1 Physical access to servers must be limited to ICT Service Division officials and all changes to servers must be made in accordance with the change management and control policies and procedure manuals.

13.2 All server users with administrative access rights must be documented.

13.3 ICT Service Division officials will use their login credentials to log on to servers at all times.

14. MONITORING

14.1 Mechanisms shall be put in place to monitor network access, failed login attempts, trends, monitor network stability, logged-out frequency etc.

14.2 Reports shall be generated monthly.

15. CLIENT DATA ACCESS

15.1 User Data folders must have permissions enabled and only the owner of the folder and files and administrators should be allowed access to these folders.

16. BREACH OF THIS POLICY

16.1 Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or

breach of contract must be reported to the Director of Financial Services which will assess its level of severity. Appropriate disciplinary action or punitive recourse may be instituted against any user who contravenes this policy.

16.2 Actions may include, but are not limited to:

16.2.1 Revocation of access to Municipal systems and ICT services;

16.2.2 Disciplinary action in accordance with the Municipal policy;

16.2.3 Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or

16.2.4 Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

17. POLICY REVIEW

17.1 The policy shall be reviewed annually by the ICT Steering Committee.

ICT PATCH MANAGEMENT POLICY

1 July 2026

TABLE OF CONTENTS

1. ABBREVIATIONS

"SWDM" refers to Swellendam Municipality.
"ICT Services Division" refers to Swellendam ICT Department and its staff members.
"Site Manager" refers to anyone appointed as the head of technical operations.
"Manager ICT Services" refers to the Head of the ICT Services Division
"COBIT" refers to Control Objectives for Information and Related Technology
"ICT" refers to Information and Communication Technology
"ITIL" refers to ICT Infrastructure Library
"SIP" refers to a Service Improvement Plan
"CRF" refers to Change Request Forms.
"Email" refers to electronic mail.
"CFO" refers to Director Financial Services.
"HOD" refers to the Manager or Head of Division.
"IP" refers to Internet Protocol
"ISO" refers to International Organization for Standardisation

2. PURPOSE OF THIS POLICY

2.1 The ICT Services Division has developed the ICT Information Security Controls Policy that shall apply to all SWDM officials, its contractors, service providers, interns, students, councillors; other authorized 3rd party entities, and every individual and/or organization and/or entity that will need the Municipality's ICT Infrastructure and Financial Systems to perform their respective duties at SWDM.

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

2.3 The purpose of the policy is to present regulations that need to be adhered to by all departments as well as all individuals who use SWDM ICT Systems.

2.4 This policy directs the implementation of appropriate security measures to ensure that information and information systems are protected in a manner commensurate with their sensitivity, value, and criticality against a variety of risks/threats or vulnerabilities such as errors, fraud, theft, embezzlement, privacy, sabotage, violence, service interruption, inception, fabrication, modification, hardware failure, industrial espionage, viruses, and natural disasters.

2.5 The Patch Management policy will minimize the security threats such as interruption, interception, modification, and fabrication of the computing systems and financial systems. The policy describes the Information Technology Services requirements for maintaining up-to-date operating system security patches on all SWDM-owned and managed workstations and servers.

3. LEGISLATIVE FRAMEWORK

3.1 The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognized ICT standards. The following legislation, among others, was considered in the drafting of this policy:

- 3.1.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- 3.1.2 Copyright Act, Act No. 98 of 1978;
- 3.1.3 Electronic Communications and Transactions Act, Act No. 25 of 2002;
- 3.1.4 Minimum Information Security Standards, as approved by Cabinet in 1996;
- 3.1.5 Municipal Finance Management Act, Act No. 56 of 2003;
- 3.1.6 Municipal Structures Act, Act No. 117 of 1998;
- 3.1.7 Municipal Systems Act, Act No. 32, of 2000;
- 3.1.8 Provincial Archives and Record Service of South Africa Act, Act No. 3 of 2005;
- 3.1.9 Provincial Archives Regulations and Guidelines;
- 3.1.10 Promotion of Access to Information Act, Act No. 2 of 2000;
- 3.1.11 Protection of Personal Information Act, Act No. 4 of 2013;
- 3.1.12 Regulation of Interception of Communications Act, Act No. 70 of 2002;
- 3.1.13 Treasury Regulations for Departments, trading entities, constitutional institutions, and public entities, Regulation 17 of 2005;
- 3.1.14 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- 3.1.15 Control Objectives for Information Technology (COBIT) 5, 2012;
- 3.1.16 ISO 27002:2013 Information technology — Security techniques Code of practice for information security controls;
- 3.1.17 King IV - Code of Governance Principles.

4. USER AWARENESS

4.1 Every councillor, employee, contractor, and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when effecting changes to SWDM ICT Infrastructure.

4.2 This policy will be sent using email to all users of ICT services and it is expected of all users to familiarize themselves with the contents and provisions of this policy.

4.3 The ICT Services Division must ensure that by requesting for changes to be effected and signing the change control form, this policy was read and understood.

4.4 Permanent Employees are to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards;

4.5 An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary Employees before they started any work for the SWDM;

4.6 The Municipality is committed to providing regular and relevant Information Security awareness communications to all Employees by various means, such as electronic updates, briefings, newsletters, etc.;

4.7 All Employees are to receive Information Security awareness training. The Information Policy must form part of all employees' induction conducted by the SWDM.

5. DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY

5.1 ICT Standard Operating Procedure.
5.2 ICT User and Network Access Policy.
5.3 SWDM Asset Management Policy.
5.4 ICT Remote Access Policy.
5.5 ICT Data Backup and Recovery Policies.
5.6 ICT Security Control Policy

6. SCOPE OF APPLICATION

6.1 The scope of this policy covers any ICT-related equipment or asset and includes and is not limited to software (Financials, GIS, OS, Utility, drivers, patches, updates, upgrades, service packs), hardware (servers, printers, desktops, laptops, scanners, 3Gs, etc), applications (office, adobe, etc), documents, plans and procedures relevant to the running, support, and maintenance of ICT Systems and Services.

6.2 This policy shall apply to all employees of SWDM, and any other person or system granted permission to use the ICT Infrastructure and Financial Systems of SWDM.

6.3 The following systems have been categorized according to management:
- 6.3.1 Microsoft Windows servers
- 6.3.2 Workstations (desktops and laptops)

7. ROLES AND RESPONSIBILITIES

7.1 All SWDM ICT Services Division are responsible to make sure that they are providing access and effect changes in compliance with the Municipality's ICT Information Security Policy. It is the responsibility of every user of ICT Infrastructure to ensure adherence to this Information Security Policy.

7.2 SWDM ICT Services is responsible for informing users of prospective changes that affect them through email and their Directors and/or Managers whichever is applicable or both.

7.3 No Employee may tamper with any security settings on any computer that may endanger the SWDM, including but not limited to the removal of screen-savers, removal of anti-virus software, etc;

7.4 Confidential Information should be shared only with other authorized persons in terms of POPIA;

7.5 Following is a list of responsibilities for software patch management:
- 7.5.1 The ICT Manager will manage the patching needs for all the financial servers on the network.
- 7.5.2 The ICT Service Provider will manage the patching needs for the Microsoft Windows servers on the network.
- 7.5.3 The ICT Server Administrators will manage the patching needs of all workstations on the network.
- 7.5.4 The ICT Manager will manage the updating and patching needs of all workstations and servers installed with the antivirus system on the network.

7.5.5 The ICT Manager will be responsible for approving the major and emergency patch management deployment requests, requested through Change Management Process.

8. WORKSTATIONS

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

8.2 Desktops and laptops may have automatic updates enabled for operating system patches. This can be the default configuration for all workstations built by SWDM. Any exception to the policy must be documented and forwarded to the ICT for review. These changes must follow a change management procedure of SWDM.

8.3 Should it be noted that any desktop and laptop update does not run automatically the ICT Services Department may manually run the updates and enable and test that updates run automatically.

9. ICT SERVERS

9.1 Servers must comply with the minimum baseline requirements that have been approved by ICT. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the ICT information assets and the data that resides on the systems.

9.2 The ICT Manager must check and install firewall upgrades and patches on a weekly basis. An obsolete firewall (one that is not supported by the vendor any longer and/or has known security vulnerabilities) must be replaced.

9.3 Any exception to the policy must be documented and forwarded to ICT for review.

10. MONITORING AND REPORTING

10.1 Active patching teams noted in the Roles and Responsibility section (7) are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Internal Audit and Management upon request.

10.2 Internal Audit and Management may conduct random assessments to ensure compliance with the policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the SWDM issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow the policy may lead to disciplinary action.

11. EXCEPTIONS

11.1 Exceptions to the patch management policy require formal documented approval from ICT Management. Any servers or workstations that do not comply with policy must have an approved exception on file with the Manager ICT Services.

12. ENFORCEMENT

12.1 Implementation and enforcement of this policy is ultimately the responsibility of the Management of ICT Services together with the Users. Deployment of such services may be enforced through the system policies, manual configurations, and Push Technology systems.

12.2 For the quality of service and assurance manual patches will be used to deploy the latest Microsoft product updates to computers running Microsoft Windows Server 2008, Microsoft Windows Server 2010, Microsoft Windows® XP, Microsoft Windows 7, 8, and Microsoft Windows 10 operating systems.

12.3 Manual patches are deployed as a precautionary measure to ensure continuity of service. This is currently the most cost-effective method and the most efficient system based on the size and simplicity of SWDM.

12.4 Other patches and updates shall follow the OEM requirements.

12.5 WSUS will be used to run updates on all the workstations and servers at SWDM.

12.6 The test environment shall be used to test patches, hotfixes, updates, service packs, etc before they are deployed on a live environment.

13. BREACH OF POLICY

13.1 Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the CFO and evaluated on its level of severity.

13.2 The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy.

13.3 Actions include, but are not limited to:

13.3.1 Revocation of access to Municipal systems and ICT services;
13.3.2 Disciplinary action in accordance with the Municipal policy; or
13.3.3 Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
13.3.4 Punitive recourse against a service provider in terms of the contract.

14. REVIEW OF POLICY

14.1 The policy shall be reviewed annually.

ICT SECURITY CONTROLS POLICY

1 July 2026

TABLE OF CONTENTS

1. ABBREVIATIONS

"SWDM" refers to Swellendam Municipality.
"ICT Services Division" refers to Swellendam ICT Department and its staff members.
"Site Manager" refers to anyone appointed as the head of technical operations.
"Manager ICT Services" refers to the Head of the ICT Services Division
"COBIT" refers to Control Objectives for Information and Related Technology
"ICT" refers to Information and Communication Technology
"ITIL" refers to ICT Infrastructure Library
"SIP" refers to a Service Improvement Plan
"CRF" refers to Change Request Forms.
"Email" refers to electronic mail.
"CFO" refers to Director Financial Services.
"HOD" refers to the Manager or Head of Division.
"BYOD" refers to Bring Your Own Device
"IP" refers to Internet Protocol
"ISO" refers to International Organization for Standardisation
"PIN" refers to Personal Identification Number
"SSH" refers to Secure Shell
"UPS" refers to Uninterrupted Power Supply
"USB" refers to Universal Serial Bus
"WPA2" refers to Wi-Fi Protected Access 2

2. PURPOSE OF THIS POLICY

2.1 The purpose of this policy is to control access and changes to the Council ICT resources and to safeguard and control SWDM ICT Infrastructure.

2.2 This policy serves to guide all who are responsible for effecting changes to ICT Infrastructure for purposes of investigation, analyzing, assessing, testing and implementing changes. This policy seeks to minimize disruption to ICT services at SWDM.

2.3 Information security ensures that the SWDM ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as the unauthorised disclosure or incorrect processing of data.

2.4 This policy ensures that the SWDM conforms to a standard set of security controls for information security in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and risks associated with the management of Information Security are mitigated.

2.5 This policy supports the Municipality's Corporate Governance of ICT Policy.

3. LEGISLATIVE FRAMEWORK

3.1 The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards. The following legislation, among others, was considered in the drafting of this policy:

3.1.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
3.1.2 Copyright Act, Act No. 98 of 1978;
3.1.3 Electronic Communications and Transactions Act, Act No. 25 of 2002;
3.1.4 Minimum Information Security Standards, as approved by Cabinet in 1996;
3.1.5 Municipal Finance Management Act, Act No. 56 of 2003;
3.1.6 Municipal Structures Act, Act No. 117 of 1998;

3.1.7 Municipal Systems Act, Act No. 32, of 2000;
3.1.8 Provincial Archives and Record Service of South Africa Act, Act No. 3 of 2005;
3.1.9 Provincial Archives Regulations and Guidelines;
3.1.10 Promotion of Access to Information Act, Act No. 2 of 2000;
3.1.11 Protection of Personal Information Act, Act No. 4 of 2013;
3.1.12 Regulation of Interception of Communications Act, Act No. 70 of 2002;
3.1.13 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005;
3.1.14 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
3.1.15 Control Objectives for Information Technology (COBIT) 5, 2012;
3.1.16 ISO 27002:2013 Information technology — Security techniques Code of practice for information security controls;
3.1.17 King IV - Code of Governance Principles.

4. SCOPE

4.1 The policy applies to everyone in the SWDM, including its 3rd party service providers and consultants.

4.2 This policy is regarded as being critical to the security of the ICT systems of the Municipality.

4.3 The policy covers the following elements of information security:

4.3.1 Security Incident Management;
4.3.2 Physical security;
4.3.3 Application security;
4.3.4 Network security;
4.3.5 Database security;
4.3.6 Change control; and
4.3.7 Software authorisation and licensing.

4.4 Aspects relating to user access, server security and data backup are covered in the ICT User Access Management, ICT Operating System Security Controls and the ICT Data Backup and Recovery policies.

5. SECURITY USER AWARENESS

5.1 Every councillor, employee, contractor and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when effecting changes to SWDM ICT Infrastructure.

5.2 This policy will be sent using email to all users of ICT services and it is expected of all users to familiarize themselves with the contents and provisions of this policy.

5.3 The ICT Services Division must ensure that by requesting for changes to be effected and signing the change control form, this policy was read and understood.

5.4 Permanent Employees are to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards;

5.5 An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary Employees before they started any work for the SWDM;

5.6 The Municipality is committed to providing regular and relevant Information Security awareness communications to all Employees by various means, such as electronic updates, briefings, newsletters, etc.;

5.7 All Employees are to receive Information Security awareness training. The Information Policy must form part of all employees' induction conducted by the SWDM.

6. GENERAL CONTROL ENVIRONMENT

6.1 The SWDM has a legal right and duty to:

6.1.1 Protect its Information Assets from internal and external information security threats;
6.1.2 Secure its network, data and communications;
6.1.3 Protect the privacy, dignity and free speech of the public and private data collected from the public;

6.1.4 Ensure that the information system is available, operational and safe;
6.1.5 Provide awareness to its employees regarding information security risks and liabilities;
6.1.6 Foster awareness of information security threats;
6.1.7 Comply with new information technology and data protection legislation; and
6.1.8 To protect the SWDM Business Information and any consumer Information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability;
6.1.9 To establish responsibility and accountability for information security in the SWDM;
6.1.10 To encourage management and Employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of information security incidents;
6.1.11 To ensure that the SWDM can continue its commercial activities in the event of significant information security Incidents.
6.1.12 To ensure the reliability of ICT services and to comply with legislation, all Municipal systems and infrastructure must be protected with physical and logical security measures to prevent unauthorised access to Municipal data.

7. DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY

7.1 ICT Standard Operating Procedure.
7.2 ICT Equipment and Allocation Policy
7.3 ICT User and Network Access Policy
7.4 SWDM Asset Management Polic
7.5 ICT Remote Access Policy
7.6 ICT Data Backup and Recovery Policy.
7.7 ICT Software Patch Policy

8. ROLES AND RESPONSIBILITIES

8.1 All SWDM ICT Services Team members are responsible to make sure that they are providing access and effecting changes in compliance with the Municipality's ICT Information Security Policy. It is the responsibility of

every user of ICT Infrastructure to ensure adherence to this Information Security Policy.

8.2 SWDM ICT Services is responsible for informing users of prospective changes that affect them through email and their Directors and/or Managers whichever is applicable or both.

8.3 All Employees must treat passwords as private and highly confidential. Employees may not disclose their own passwords to anyone. Non-compliance with this policy could result in disciplinary action;

8.4 Employees may not attempt to discover another person's password;

8.5 All Employees are responsible for all system activity conducted under their User ID;

8.6 No Employee may tamper with any security settings on any computer that may endanger the Municipality, including but not limited to removal of screen-savers, removal of anti-virus software, etc;

8.7 Employees may not attempt to illegally gain access to another user's files and/or another site's computer facilities;

8.8 All software and/or licensing copyright requirements must be strictly adhered to by all Employees;

8.9 No new Software packages or downloads must be installed by any employee. Only the ICT Services Division is allowed to install software or any other applicable downloads.

8.10 Confidential Information should be shared only with other authorised persons;

8.11 The ICT Manager and or delegate must sign for the receipt of all computer equipment and or goods. They are to ensure that, by signing for them, they are considered to be verifying the correct quantity, quality and condition of the goods according to the order issued;

8.12 Employees must sign for the receipt of computer equipment and or goods provided at their workstations. They are to ensure that, by signing

for them, they are considered to be verifying the quantity, quality and condition of the goods issued;

8.13 Only authorised persons may sign for work done by third parties;

8.14 Only the ICT Manager per the delegated authority may order ICT infrastructure and computer equipment on behalf of the Municipality;

8.15 Telephone enquiries for Sensitive or Confidential Information are to be referred to management. Only authorised persons may disclose Information classified for Public Information in terms of the POPIA Act;

8.16 All data and information not in the public domain, relating to the SWDM and its Employees, must remain confidential at all times;

8.17 The playing of games on office PCs or laptops is prohibited; and

8.18 Using the Municipality's computers for personal/private business is strongly discouraged.

9. PHYSICAL SECURITY

9.1 The ICT Manager must take reasonable steps to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery.

9.2 ICT hardware under control of the ICT function must be hosted in server rooms or lockable cabinets. Server rooms must be of solid construction and locked at all times.

9.3 The security alarm company must provide a user access list once a month for the access to be monitored and verified. The user access list must be available to the Internal Auditor upon request.

9.4 All server rooms must be equipped with air-conditioning, UPS and fire detection and suppression. (fire detection to be installed later)

9.5 A maintenance schedule must be created and maintained for all ICT hardware under the control of the ICT department. Maintenance activities must be recorded in a maintenance register.

9.6 A call logging system must be in place to control any changes or maintenance in the ICT department.

9.7 Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.

9.8 Cabling must be neat and protected from damage and interference.

9.9 No ICT equipment may be removed from the server room or offices without prior authorisation from the ICT Manager.

9.10 All hardware owned by the Municipality must be returned by employees and service providers when no longer needed or on termination of their contract.

9.11 All data and software on hardware must be erased before disposal or re-use.

9.12 Any hardware that carries data that can be carried off-site (e.g. laptop computers, removable hard disks, flash drives etc.) must be protected with encryption.

9.13 ICT hardware and software must be standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the Municipality.

9.14 The off-site location, used to store backup data media, must be protected with the following physical security measures: (To be implemented once established)

9.14.1 Building of solid construction;
9.14.2 Physical access control;
9.14.3 Fire detection and suppression; and
9.14.4 Environmental conditions adhere to vendor recommendations for the storage of media.

10. DATABASE SECURITY

10.1 The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need

this access. Officials who use applications may not have these rights to the application's databases.

10.2 The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.

10.3 The ICT Manager with CFO must approve all instances where Officials have edited or executed access to databases.

10.4 The ICT Manager must review database rights and permissions quarterly. Excessive rights and permissions must be removed.

11. NETWORK SECURITY

11.1 The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.

11.2 The ICT Manager must implement a firewall between the Municipal network and other networks.

11.3 The ICT Manager must limit administrator access to the firewall and user accounts must have strong passwords of at least 8 characters with a combination of alpha-numeric characters and symbols. Remote firewall administration is only allowed using SSHv2 from the internal network.

11.4 The ICT Manager must check and install firewall upgrades and patches on a weekly basis. An obsolete firewall (one that is not supported by the vendor any longer and/or has known security vulnerabilities) must be replaced.

11.5 The ICT Manager must document the firewall rulesets and configuration settings. The rulesets and configuration settings must be reviewed quarterly to ensure that it remains current (i.e. remove unused services) and that services that expose the Municipality to security risk are reviewed continuously.

11.6 The ICT Manager must configure the firewall to block all incoming ports unless the service is required to connect to a server on the internal network (e.g. port 80 and port 443 for web servers). When an incoming

port is allowed, the service may only connect to the specific servers on the internal network. Internal IP addresses may not be visible outside of the internal network.

11.7 The ICT Manager must approve all open incoming ports. Only absolutely necessary requests and with consideration of the associated security risks must be approved.

11.8 The system administrators must set the firewall to block intrusion attempts and to alert the ICT Manager when additional action needs to be taken. The ICT Manager must raise an incident and deal with the root causes of the event.

11.9 The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally on separate network domains.

11.10 The ICT department must scan the entire network with security software on a monthly basis to detect security vulnerabilities. The scans must be performed from the Internet, as well as from the internal network.

11.11 Officials and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.

11.12 System administrators must install personal firewalls on laptops and personal computers. Officials may not disable these firewalls. Officials must choose to deny a specific address when prompted by the personal firewall unless approved by ICT.

11.13 The ICT department must ensure that all inactive network points are disabled.

12. E-MAIL AND INTERNET

12.1 The ICT Manager must make all users aware of the safe and responsible use of e-mail and Internet services. E-mail and the Internet should only be used for official use. Personal usage can be permitted if it does not interfere with job functions. E-mail and the Internet may not be used for any illegal or offensive activities.

12.2 Officials and the ICT department may not use Internet cloud services (e.g. Google Drive, Gmail, Dropbox etc.) for official purposes unless approved by the ICT Steering Committee.

12.3 The transmission of Sensitive and Confidential Information is to be Authenticated by the use of Digital Signatures whenever possible;

12.4 Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible Viruses or other Malicious Code;

12.5 Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all Employees as detailed in the Municipality Records Management Policy;

12.6 ICT Service Division responsible for setting up internet/intranet access must ensure that any access restrictions pertaining to the data in source systems are also applied to access from the SWDM Intranet;

12.7 ICT Service Division is responsible for setting up Internet access are to ensure that the Municipality's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured Firewall.

12.8 Unsolicited e-mail is to be treated with caution and not responded to;

12.9 The ICT Services Division is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security Incidents;

12.10 Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. the Municipality's ICT Services Division must ensure that Employees are made aware of the appropriate settings for the software concerned;

12.11 Information obtained from Internet sources should be verified before being used for municipal purposes;

12.12 The website is an important marketing and information resource for the SWDM and its safety from unauthorised intrusion is a top priority. Only

qualified authorised persons may be developed and amend the website with all changes being documented and reviewed;

12.13 The Municipality's ICT Services will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by Employees. Reports of attempted access will be scrutinised by management regularly; and

12.14 Computer files received from unknown senders are to be deleted without being opened.

13. TELEPHONE AND FAX

13.1 Conference calls are only permitted if Employees are aware of the Information Security issues involved;

13.2 Video conference calls are only permitted if Employees are aware of the Information Security issues involved;

13.3 All parties are to be notified in advance whenever telephone conversations are to be recorded;

13.4 Any fax received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission;

13.5 The identity of persons requesting Sensitive or Confidential Information over the telephone must be verified, and they must be authorised to receive it in terms of the POPIA;

13.6 Fax covering pages must be used on all manual faxes.

14. DATA MANAGEMENT

14.1 Sensitive, Private, or Confidential Information may only be transferred across networks, or copied to other media when the confidentiality and integrity of the data can be reasonably assured;

14.2 Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need;

14.3 The integrity and stability of the SWDM databases must be maintained at all times;

14.4 The use of removable media disks e.g. flash drives and CD-ROMs must be scanned before use for viruses and other malware.

14.5 Existing directory and folder structures may only be amended by the ICT Manager with the appropriate authorisation. Access restrictions to such directories should be applied as necessary to restrict unauthorised access.

14.6 The archiving of documents must take place with due consideration for legal, regulatory and municipal issues with liaison between technical and business Employees as detailed in the Municipality Records Management Policy.

14.7 The Information created and stored by the Municipality's information systems must be retained for a minimum period that meets both legal and municipal requirements as detailed in the Municipality Records Management Policy;

14.8 Only authorised employees may access Private, Sensitive or Confidential Information on projects owned or managed by the Municipality or its Employees;

14.9 Consumer Information may only be updated by authorised Employees;

14.10 Consumer data is to be safeguarded using a combination of technical Access Controls and robust procedures, with all changes supported by journals and internal audit trails; These are usually dealt with by other Departments and Directorates and due diligence should be taken in controlling access.

14.11 All users of information systems whose job function requires them to create or amend data files must save their work on the system regularly in accordance with best practices, to prevent corruption or loss through system or power malfunction.

15. WIRELESS NETWORKS

15.1 System administrators must configure all wireless networks to the following standard:

15.1.1 WPA2 security protocol or better;

15.1.2 Password strength of at least 8 characters with a combination of alphanumeric characters and symbols;

15.1.3 The latest firmware must be installed; and

15.1.4 Default system usernames and passwords must be removed.

16.2 Officials may not establish wireless networks attached to the internal network without the consent of the ICT Manager. All wireless networks must adhere to the secure configuration standard.

16. MOBILE DEVICES AND OWN HARDWARE (BYOD)

16.1 The ICT Manager in consultation with the CFO must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.

16.2 The ICT Service Division must ensure that all mobile devices must be protected with a PIN.

17. INFORMATION SYSTEMS

17.1 Access to all systems must be authorised by the owner of the system and such access, including the appropriate Access Rights (or privileges), must be recorded in an Access Control List.

17.2 Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised;

17.3 Access to Operating System commands is to be restricted to those persons who are authorised to perform systems administration/management functions. Even then, such access must be operated under Dual Control requiring the specific approval of the Information Security Officer;

17.4 The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. Passwords shall not be shared with any other person for any reason;

17.5 Access controls are to be set at an appropriate level which minimises information security risks yet also allows the SWDM activities to be carried out without undue hindrance;

17.6 Access to information systems is to be logged and monitored to identify potential misuse of systems or Information;

17.7 Access to Information and documents is to be carefully controlled, ensuring that only authorised employees may have access to Sensitive Information; and

17.8 Access controls for Sensitive Information or high-risk systems are to be set in accordance with the value and classification of the Information Assets being protected.

18. SOFTWARE

18.1 The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased information security risks associated with such projects are mitigated using a combination of procedural and technical control techniques;

18.2 Only ICT Service Division are to install software on the SWDM systems; and

18.3 The disposal of software should only take place when it is formally agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.

18.4 When unauthorised software is discovered on a user's computer is deleted without notice. That deletion will be recorded on the Track-IT and Change Management System.

18.5 Management must ensure that proper Segregation of Duties applies to all areas dealing with systems development, systems operations, or systems administration.

18.6 The use of live data for testing new systems or system changes may only be permitted where adequate controls for the security of the data are in place;

18.7 All new and enhanced systems must be fully supported at all times by comprehensive and up-to-date documentation.

18.8 New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

18.9 The ICT Manager must retain a record of all licenses owned by the SWDM.

18.10 The ICT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.

18.11 An approved software list must be maintained by the ICT Manager.

18.12 Employees may not install or change the software on their computers.

19. SOFTWARE PATCH MANAGEMENT

19.1 Patch Management will minimize the security threats such as interruption, interception, modification and fabrication of the computing systems and financial systems.

19.2 The ICT Manager must develop a patch management policy that describes the Information Technology Services requirements for maintaining up-to-date operating system security patches on all SWDM-owned and managed workstations and servers.

19.3 Following is a list of responsibilities for software patch management:

19.3.1 The ICT Manager will manage the patching needs for all the financial servers on the network.
19.3.2 The ICT Service Provider will manage the patching needs for the Microsoft Windows servers on the network.
19.3.3 The ICT Server Administrators will manage the patching needs of all workstations on the network.

19.3.4 The ICT Manager will manage the updating and patching needs of all workstations and servers installed with the antivirus system on the network.

19.3.5 The ICT Manager will be responsible for approving the major and emergency patch management deployment requests, requested through Change Management Process.

20. PASSWORD MANAGEMENT

20.1 Authorised Users are responsible for ensuring that their individual passwords are created and managed in accordance with the ICT User and Network Access Policy.

20.2 The minimum password length is 8 characters.

20.3 The ICT password history system must keep up to ten (10) previous passwords.

20.4 All authorised users will be required to change their passwords every 42 days.

20.5 Any password that is suspected to have been compromised must be changed immediately and the user must inform ICT services immediately.

20.6 If a user forgets their password, a request to change the password form must be completed and submitted to ICT Services Division.

20.7 The ICT Services Division will provide a temporary password to reset the user password. The user will be requested to insert a new password.

20.8 All system-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

20.9 All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

20.9.1 When a user retires, resigns, is reassigned, released, dismissed, etc.

20.9.2 Contractor/temporary workers account, when no longer needed to perform their duties or at the end of their term.

20.10 Do not share passwords with anyone, Here is a list of "do not's"

1.1.1. Don't reveal a password over the phone to anyone;

20.10.1 Don't reveal a password in a mail message;

20.10.2 Don't reveal a password to the boss;

20.10.3 Don't talk about a password in front of others;

20.10.4 Don't hint at the format of a password (e.g., "my family name");

20.10.5 Don't reveal a password on questionnaires or security forms;

20.10.6 Don't share a password with family members;

20.10.7 Don't reveal a password to a co-worker while on vacation;

20.10.8 Don't write passwords down and store them anywhere in your office;

20.10.9 Don't store passwords in a file on ANY computer system unencrypted;

21. INVALID LOGIN ATTEMPTS

21.1 Invalid login attempts occur when the username or password is typed in incorrectly.

21.2 Usernames and passwords will be locked out from the network after three invalid login attempts and may only be reset after the completion of a password ticket.

21.3 A screen timeout of 600 seconds, if no valid lock-in was registered.

21.4 Third-Party Systems which are administered by the systems providers will determine their account lockout threshold.

22. TRANSFER OF INFORMATION

22.1 The ICT Manager must ensure that classified information may only be transmitted over external networks using encryption.

22.2 Officials may not use personal storage devices (e.g. USB memory sticks or portable hard drives) to store Municipal data. When required for

official purposes, and the data is confidential, these devices must be encrypted by the ICT Manager.

23. MONITORING

23.1 The CFO authorises the monitoring of Municipal systems by the ICT Manager.

23.2 Municipal officials must be made aware that the network is being monitored to ensure network security, to track the performance of the network and systems, and to protect the network from viruses.

23.3 Any e-mail, Internet and other network services may be monitored by the ICT Manager.

24. SECURITY INCIDENTS MANAGEMENT

24.1 All Municipal users must report actual or suspected security breaches or security weaknesses to the ICT Manager or the delegated authority.

24.2 The ICT Manager must record all information regarding security incidents.

24.3 The ICT Manager must review all the information security incidents on a quarterly basis to ensure that the root cause of the problems is addressed.

24.4 Investigations into security incidents may only be carried out by the ICT Manager or a nominated person.

24.5 The Protection of Personal Information Act, Act No. 4 of 2013 prescribes that the Regular and the person affected by the breach must be notified in the event of a breach of personal information.

24.6 Employees are expected to remain vigilant for possible fraudulent activities.

24.7 The ICT Manager must report all open incidents and actions against open incidents to the CFO and wealnesses are reviwed and monitored weekly.

24.8 The ICT helpdesk shal provide feedback to individuals who reported the security incident and notify them of results.

25. CHANGE CONTROL

25.1 All changes to Municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable ICT service delivery to the Municipality, without impacting the stability and integrity of the changing environment.

25.2 Corrections, enhancements and new capabilities for applications and infrastructure will follow a structured change control process.

25.3 An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterwards. Emergency changes are only reserved for fixing errors in the production environment that cannot wait for more than 48 hours.

25.4 Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software etc.) must follow the help-desk processes designed to deliver ICT services in the most effective way.

25.5 Recurring operational tasks are excluded from the structured change control process.

25.6 The following additional rules for change control must be adhered to. In some cases this may not be cost-effective or technically possible, in which case the ICT Steering Committee has to review and approve alternative controls:

25.6.1 The same person who performs the change may not implement the change.
25.6.2 Systems must have a development environment where testing is conducted to avoid testing in the production environment.

25.6.3 If a vendor performs the change, the Municipality must also test the change.

25.6.4 The data inside a database may not be edited, except through an approved application front-end. This excludes internal system processes or interfaces, or work required to convert data during system implementation.

25.6.5 Commercial software must be selected after considering information security requirements.

25.6.6 The affected user's willingness to change must always be considered when documenting all that can go wrong with the change.

25.6.7 Any system published on the Internet or a mobile platform must be reviewed by security specialists before being deployed.

25.7 The ICT Manager must record all change requests across the Municipality in a central tool, file server or spreadsheet. This implies that changes performed by ICT and those changes requested by the business from vendors, without ICT involvement, must be recorded together.

25.8 The ICT Manager must create a weekly report which lists all of the unapproved change requests, active change requests, cancelled change requests and completed change requests. The report must be reviewed, and actions taken, to ensure that:

25.8.1 Change requests receive sufficient attention;

25.8.2 The change control process is being followed for all known changes;

25.8.3 Trends across change requests, that indicate systemic problems in the ICT environment, are identified and require more permanent fixes.

26. HANDLING OF FORENSIC EVIDENCE

26.1 Proper handling of digital forensic evidence is crucial to maintaining its integrity and ensuring it can be used effectively in investigations and court proceedings.

26.2 The key steps in this process are:

26.2.1 Identification of potential digital evidence and documenting its location and condition. It's important to prioritize evidence based on its volatility and value;
26.2.2 Collection of digital devices and data systematically. This can involve both static acquisition (collecting data from powered-off devices) and live acquisition (collecting data from running systems);
26.2.3 Creating a duplicate copy of the digital evidence without altering the original data. This is done using tools like write blockers to prevent any changes during the copying process;
26.2.4 Ensuring that the digital evidence remains unchanged and is stored securely. This includes maintaining a clear chain of custody to document every person who handles the evidence;
26.2.5 Conducting a thorough examination of the evidence using forensic tools and techniques. This step should be performed by qualified professionals to ensure the results are reliable;
26.2.6 Documenting the findings in a clear and accurate manner, including any limitations or uncertainties in the analysis;

27. BREACH OF POLICY

27.1 Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the CFO and evaluated on its level of severity.

27.2 The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy.

27.3 Actions include, but are not limited to:

27.3.1 Revocation of access to Municipal systems and ICT services;
27.3.2 Disciplinary action in accordance with the Municipal policy; or
27.3.3 Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
27.3.4 Punitive recourse against a service provider in terms of the contract.

28. REVIEW OF POLICY

25.1 The policy shall be reviewed annually.

ICT Steering and mSCOA Committee Terms of Reference

1 July 2026

Table of Contents

1. ABBREVIATIONS

1.1 "ICT" refers to Information Communication Technology.
1.2 "King IV" refers to King Code of Corporate Governance
1.3 "Municipality" refers to the Swellendam Municipality.
1.4 "The Committee refers to ICT Steering Committee"
1.5 "mSCOA refres to Municipal Regulation on Standard Chart of Accounts"

2. BACKGROUND

2.1 The role of the Committee has evolved over time with ever-changing information technology, to ensure that the municipality ICT services has the right product solution, applications, controls and systems in place to support the municipality.

2.2 The vital role of ICT can no longer be ignored by the municipality and it has become critical that the municipality focus on ICT governance. The role of the Committee is not to focus on a single department/division but concentrate on the Information and Communication Management function that permeates the entire organization.

2.3 The Final King IV was released on 1 November 2016, by the Institute of Directors in Southern Africa and the King Committee and set the following governance principle relating to ICT:

"The council should govern technology and information in a way that supports the municipality in setting and achieving its strategic objectives."

2.4 In line with the recommended practices of King IV, the Committee focuses on issues such as communication with stakeholders, data security and integrity, reviewing of ICT related policies and ensuring the ICT infrastructure is aligned to the strategy.

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

2.6 It is apparent that the need for an ICT governing body is not just a legal requirement, but it is a necessity within the municipality.

3. LEGISLATIVE REQUIREMENTS

This includes inter alia the:

3.1 Electronic Communications Act 36 of 2005
3.2 Electronic Communications Security (PTY) Ltd Act 68 of 2002
3.3 Telecommunications Act 103 of 1996
3.4 State Information Technology Amendment Act 38 of 2002
3.5 Promotion of Access to Information Act 2 of 2000
3.6 Municipal Finance Management Act, 2003

3.7 Municipal Systems Act, 2000
3.8 Copyright Act 98 of 1978
3.9 National Archives and Records Act 43 of 1996
3.10 Protection of Personal Information Act 4 of 2013
3.11 King Code of Government Principles (King IV), 2016
3.12 Municipal Regulation on Standard Chart of Accounts, R312, 2017
3.13 Any other applicable legislation, regulation or policy

4. PURPOSE

4.1 The purpose of this Terms of Reference is to establish an ICT Steering and mSCOA Committee responsible for governance and accountability over the Municipality's ICT and mSCOA functions, ensuring compliance with applicable legislation and alignment of ICT investments with the Municipality's strategic objectives and mSCOA requirements.

5. FUNCTIONS OF THE ICT STEERING COMMITTEE

5.1 The Committee will advise, in terms of an oversight role, to Management and/or Council on all matters relating to ICT and mSCOA requirements and be responsible for the following:

5.1.1 Ensuring that ICT strategies are aligned with National and Provincial Government directives and policy priorities;

5.1.2 Ensure compliance to the Municipality's strategic and corporate objectives, service delivery priorities, budget implementation plans, and mSCOA compliance requirements.

5.1.3 Prioritizing strategies and risks as high, medium and low, in consultation with the responsible Directorate, to provide a true indication of the areas that need to be addressed first;

5.1.4 The investigating, considering and prioritizing of high level and/or impact ICT projects;

5.1.5 Prepare and review the ICT budget and make recommendations to the Budget Office;

5.1.6 Reviewing and recommending ICT policies, procedures and standards for use by the Municipality, including the ICT governance framework;

5.1.7 Determine and monitor ICT security policies and practices on an ongoing basis to ensure relevance;

5.1.8 Review and recommend Service Level Agreements of ICT services;

5.1.9 Managing ICT risks and change management;

5.1.10 Fusing the ICT and business strategies, goals, and resources, and achieving competitive advantage through ICT.

5.1.11 Review all audit and assurance reports conducted by Internal Audit; the Auditor-General of South Africa or any independent assurance provider and make recommendations to management on these reports

5.1.12 Moitor succesful implementation of mSCOA which includes amongst other:

5.1.12.1 Review and approve the mSCOA Roadmap;
5.1.12.2 Review the mSCOA project risks;
5.1.12.3 Consider impact of mSCOA on the municpality business processs;
5.1.12.4 Ensure assessment of the current agreements with infrastructure and software service providers for consideration in planning the way forward;
5.1.12.5 Ensure that due diligence and project management were followed when financial system was changed;
5.1.12.6 Evaluate and report on the adequacy and effectiveness of mSCOA project risk process.

6. COMPOSITION AND TERM OF OFFICE OF THE COMMITTEE

6.1 The membership of the Committee should be appropriate to the size and the complexity of the Municipality. The members of the committee are constituted by different Municipal directorates.

6.2 Membership of the Committee comprised of the following:

6.2.1 Director Financial Services as Chairperson or nominated by the municipal manager;
6.2.2 One representative from each directorate, nominated by the Director of each directorate, with accompanying secondi;
6.2.3 A representative from the procurement office, nominated by the SCM Manager;
6.2.4 A representative from Internal Audit, nominated by Chief Audit Executive;
6.2.5 A representative from the human resources, nominated by the HR Manager.

6.3 Co-opted members of the Committee comprised of the following:

6.3.1 System Administrator ICT;
6.3.2 A representative from the ICT Service provider;
6.3.3 Admin clerk financial services.

6.4 The term of office for the Committee members will be concurrent with the Municipal Financial year. Each member will be appointed for a 3-year term and may be re-

appointed. Departmental directors can also nominate new representatives, as and when required.

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

6.6 Members of the Committee are subject to the Municipal Code of Conduct.

7. MEETINGS OF THE COMMITTEE

7.1 The Committee shall meet at least every quarter of the financial year.

7.2 Where it is not possible to meet at any quarter a special ICT Steering Committee meeting may be arranged to deal with urgent matters that would have been dealt with in the previous quarter.

7.3 Additional meetings will be convened when necessary.

7.4 For every meeting, the decisions and recommendations will be finalized through the consensus of the committee members.

7.5 The timing of these meetings should complement both organisation planning cycle requirements and ongoing review processes. For a committee meeting quorum to be achieved, 50% (four) of the members must be present.

7.6 Minutes must be taken of all meetings, preferably by Committee Services, and distributed electronically to all members within fourteen (14) days.

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

7.8 Agenda items should be sent to the ICT Manager, or nominated member, at least seven (7) days before the scheduled meeting.

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

7.10 Minutes of the meeting must be submitted to the Municipal Manager and Audit Committee.

8. REVIEW OF THE COMMITTEE TERMS OF REFERENCE

8.1 The content of this terms of reference will be reviewed by the Committee on an annual basis and only if major changes are required, will it be approved by Council, as and when required, to reflect the current stance on ICT within the Swellendam Municipality.

ICT STRATEGIC PLAN

1 July 2026

TABLE OF CONTENTS

1) BACKGROUND

The Swellendam Municipality, has during its IDP development processes for the period of 2022 to 2027, committed to enhancing service delivery and engagement through active citizenry.

The Municipality has committed to improving efficiency and effectiveness in the manner in which it delivers services to its citizens, which includes the manner through which it administers its daily activities. Therefore, the municipality has identified ICT as an enabler for the delivery of the IDP objectives on its mandate.

This ICT Strategic Plan seeks to enhance the maturity of the municipalities ICT environment by identifying key initiatives and focus areas to be delivered by the municipality's ICT environment. As such projects will be identified through an ICT architecture roadmap and implementation plan which will be delivered over a five (5) year cycle, and will be reviewed annually to ensure efficacy.

The ICT Strategic Plan is a tool to:

a) Assist the ICT Steering Committee to understand the complexity of managing information and technology within local government;

b) Encourage local governments to improve their ICT capability;

c) Ensure ICT is adequately managed to support all aspects of local government operations.

The overall aim of the Strategic Plan is to ensure that ICT

a) Provide a service which is of the highest quality and is responsive to the demands of the workforce of the Swellendam municipality and the Swellendam community;

b) Is thoroughly effective and efficient in the use of available resources;

c) Deliver the highest standards of professional service, involving everyone in the decision-making process, and seeking constantly to improve the working lives of all staff;

d) Adhere to the legal framework provided for in the legislations and/or policies of the Municipality through continuing professional development; and

e) Maximise available resources, and the efficiency with which they are used.

2) PURPOSE OF THE ICT STRATEGIC PLAN

The ICT Strategic Plan sets out the key components that need to be considered in managing an organisation's information resources. It represents the key elements and their relationships, that might be expected in an "ideal" environment.

The ICT Strategic Plan is not a legislative prescribed document but rather a strategic tool that the administration uses to plan, manage, monitor and review the organisation's information technology tools more effectively and efficiently for optimal sustainability.

3) LEGISLATIVE STRATEGIC DIRECTION

This strategy was developed with the legislative environment in mind, as well as to leverage internationally recognized ICT standards.

The following legislation, among others, govern the local government sphere:

a) Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
b) Municipal Finance Management Act, Act No. 56 of 2003.
c) Municipal Structures Act, Act No. 117 of 1998.
d) Municipal Systems Act, Act No. 32, of 2000.
e) Municipal Demarcation Act, Act 27 of 2000
f) Municipal Property Rates Act, Act 6 of 2004
g) National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
h) Promotion of Access to Information Act, Act No. 2 of 2000.
i) Protection of Personal Information Act, Act No. 4 of 2013.

4) ICT OBJECTIVES

ICT Objectives for the Information Communication Technology department is:

"To plan, coordinate and render ICT services to the municipality to ensure efficient operations and support services in terms of the ICT strategy and plan."

5) ICT GOVERNANCE

The King IV Report set the following governance principle relating to ICT:

"The council should govern technology and information in a way that supports the municipality in setting and achieving its strategic objectives."

IT governance is the set of processes that ensure the effective and efficient use of Information Communication Technology (ICT) in enabling an organization to achieve its goals.

The corporate governance of ICT places a very specific responsibility on the Council and Management within a municipality to ensure that the decision-making process for ICT-related investments and the operational efficiencies of the municipality's ICT environments remain transparent and upheld. This accountability enables the municipality to align the delivery of ICT services with the municipality's Integrated Development Plans and strategic goals.

6) STRUCTURE OF THE ICT ENVIRONMENT

The Director Financial Services are responsible for the municipality's ICT environment, supported by an ICT Manager, ICT Steering Committee and Co-sourced Service Provider.

a) ICT Unit

Information and Communication Technology (ICT) forms part of the Directorate of Financial Services. The ICT Department is responsible to plan, coordinate and render ICT services to the municipality to ensure efficient operations and support services in terms of the ICT strategy and policies.

The functions of the ICT Department are to:

(i) Develop and implement an ICT strategy and policy for the Municipality;
(ii) Provide operations and support services;
(iii) Research, develop and maintain ICT systems;
(iv) Ensure network connectivity so that users have access to the network;
(v) Install ICT equipment and appropriate software programmes to ensure the availability of services and licensing;
(vi) Provide expert advice regarding the acquisitions of maintenance of ICT equipment and system;
(vii) Maintain ICT systems to ensure the efficient operations of all systems;
(viii) Safeguard all electronic data and/or information of the municipality;
(ix) Ensure access and security control to the municipality ICT network.

b) ICT Steering Committee

All ICT-related Services and Systems are governed by the Swellendam ICT Steering Committee. The ICT Steering Committee oversees, monitors and directs all ICT-

related initiatives to ensure ongoing alignment with Strategic Directives as stated in the IDP.

The membership of the Committee should be appropriate to the size and the complexity of the Municipality. The members of the committee are constituted by different Municipal directorates. Membership of the Committee comprised of the following:

(i) Director Financial Services as Chairperson or nominated by the municipal manager;
(ii) One representative from each directorate, nominated by the Director of each directorate, with accompanying secondi;
(iii) A representative from the procurement office, nominated by the SCM Manager;
(iv) A representative from Internal Audit, nominated by Chief Audit Executive;
(v) A representative from human resources, nominated by the HR Manager.

Co-opted members of the Committee comprised of the following:

(i) Manager ICT;
(ii) A representative from the ICT Service provider;
(iii) Admin clerk financial services.

The term of office for the Committee members will be concurrent with the Municipal Financial year. Each member will be appointed for a 3-year term and may be re-appointed. Departmental directors can also nominate new representatives, as and when required.

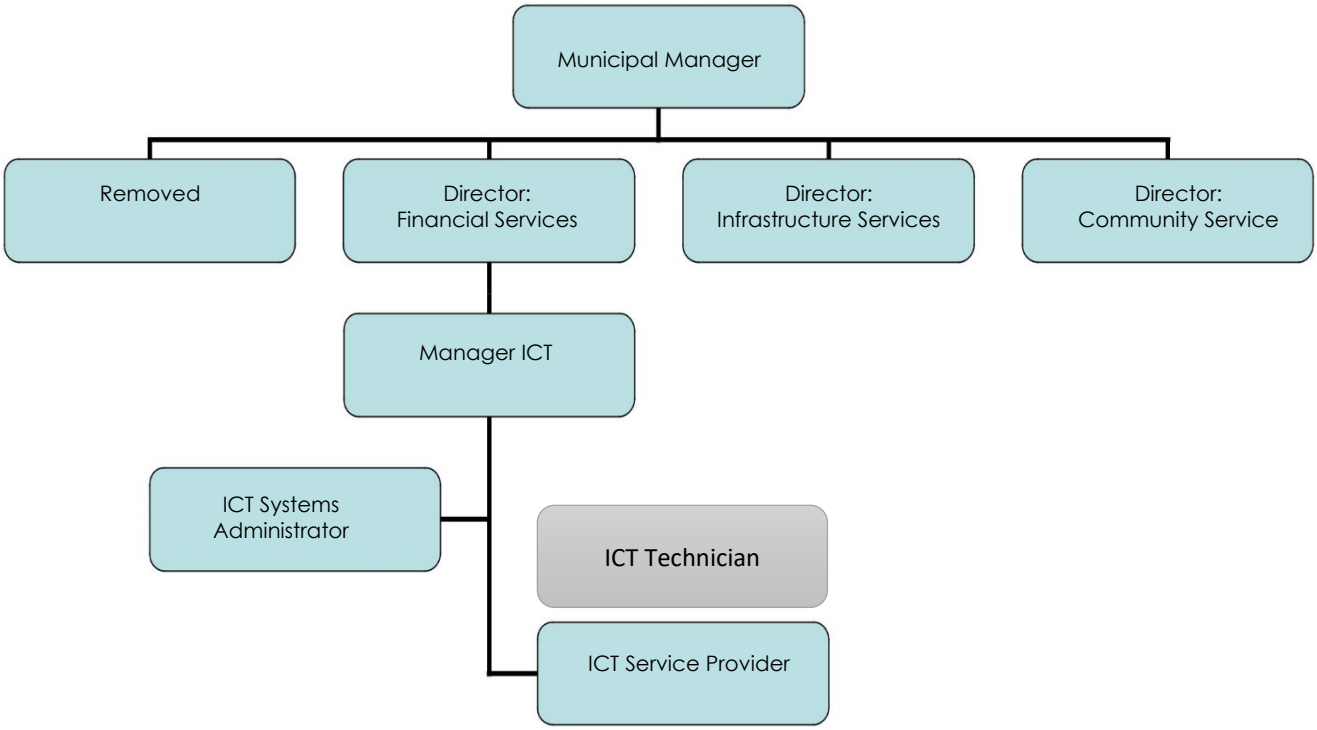
The Municipal Manager must appoint the Committee members through a formal appointment letter that indicates the term of membership.

Members of the Committee are subject to the Municipal Code of Conduct.

The Chairperson may invite other persons to attend meetings as required. In the absence of a member, his/her delegate may attend the meeting on behalf of the member. In the absence of the chairperson, the members shall amongst themselves elect an acting chairperson to chair the meeting.

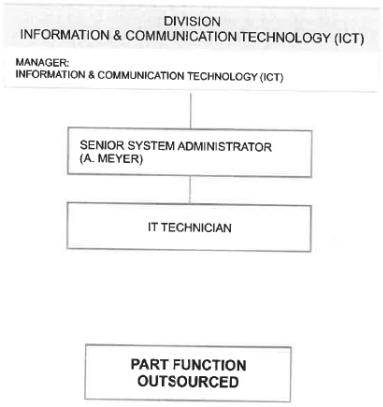
The Committee shall meet at least every quarter of the financial year. Where it is not possible to meet at any quarter a special ICT Steering Committee meeting may be arranged to deal with urgent matters that would have been dealt with in the previous quarter.

c) Organisational Structure



CONFIDENTIAL

SWELLENDAM LOCAL MUNICIPALITY
FINAL MICRO STRUCTURE
31 MARCH 2026



Page 9 of 44

7) RISK MANAGEMENT

The management of risks is a cornerstone of ICT Governance, ensuring that the strategic objectives of the business are not jeopardised by ICT failures. ICT-related risks are increasing, and the impact on the organisation of an ICT failure, be it an operational crash, security breach or a failed project, can have devastating consequences.

However, managing ICT risks and exercising proper governance is a challenging experience for business managers faced with technical complexity, dependence on an increasing number of service providers, and limited reliable risk monitoring information.

Therefore, the ICT risk of the municipality should be managed by:

(i) Ascertaining that there is transparency about the significant risks to the municipality and clarifying the risk-taking or risk-avoidance policies.
(ii) Ensure that the system of internal control put in place to manage risks has the capacity to generate cost efficiency.
(iii) Ensure that risk management is embedded in the operation of the municipality, responds quickly to changing risks and reports immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).

8) PLANNING AND RESOURCE GUIDELINES

The ICT Budget is submitted to the finance department by the ICT Manager and ICT Steering Committee for consideration and oversight. The ICT budget forms part of the municipality's annual budget which is presented to the Council for approval.

ICT aims to follow a basic approach to identifying and implementing projects inclusive of:

(i) Concept and initiation
(ii) Definition and planning (scope and budget; communication, risk management)
(iii) Execution
(iv) Testing and review
(v) Reporting and closing of the project

9) ICT SERVICES PROVIDED IN THE MUNICIPALITY TO DIRECTORATES

a) Ongoing Services

(i) Network architecture
(ii) Virtualization
(iii) Internet access
(iv) Remote access to the network when working out of the office
(v) E-mail Services, contacts and groups
(vi) File server and storage
(vii) Printing/copying/faxing
(viii) Desktop & laptop support and installation
(ix) Telephony (VOIP) and audio visual
(x) User access
(xi) ICT equipment and WIFI
(xii) ICT security
(xiii) VPN access
(xiv) Backup management

b) Systems

(i) Access to Samras Financial System
(ii) Access to Self-Service Samras Module
(iii) Access to Ignite
(iv) Access to Eunomia
(v) Access to Colaborator
(vi) Access to Collaborator Citizen App
(vii) Assess to GIS

c) Software Management

(i) Install and update Microsoft Windows
(ii) Install and update Microsft Office

(iii) Install and update Kaspersky Software
(iv) Install and update SSL Certificate
(v) Install and update Zimbra
(vi) Install and update Zoom
(vii) Install and update Adobe

10) KEY ICT FOCUS AREAS & TIMELINES

The municipality has to ensure that it has viable ICT strategies to meet both goals and challenges faced by the municipality to conduct its business effectively, efficiently and quickly. These strategies may be classified as short-term, medium-term and long-term to ensure the continuity of the municipality. This simply means the municipality has to list possible projects that will support the day-to-day activities of the municipality for the betterment of municipal service delivery. The ICT strategies must be directly linked to the Integrated Development Plan of the municipality and are reviewed annually if needed.

The projects/activities of the ICT Strategic Plan for 2025/2026 MTREF is tabled below:

Nr	Activity	Type of Project	Risk	Year 1 2026/2027	Year 2 2028/2029	Year 3 2029/2030
1.	Establish Disaster Recovery Site at Garden Route	New	High	Bi-Annually Testing	Maintain	Maintain
2.	Roll-out Microsoft 365 ad-hoc Licence to senior personal and staff • Web based student licences	Maintain	High	Implement	Implement	Implement
3.	Review ICT Policies per register.	Maintain	Medium	Maintain	Maintain	Maintain
4.	Implement ICT Budget	Maintain	Medium	Maintain	Maintain	Maintain
5.	Renewal of Telephone Contract	Maintain	Medium	Maintain	Maintain	Maintain
6.	Renewal of Printer / Copier Contract.	Maintain	Medium	Maintain	Maintain	Maintain

Nr	Activity	Type of Project	Risk	Year 1 2026/2027	Year 2 2028/2029	Year 3 2029/2030
7.	Upgrade firewall software.	Maintain	High	Maintain	Maintain	Maintain
8.	Renewal of ICT Tender.	Maintain	High	Maintain	Maintain	Maintain
9.	Improve and implement the New ICT Governance Policies and Procedures.	New	High	Implement	Implement	Maintain
10.	Review User Access.	Maintain	Medium	Maintain	Maintain	Maintain
11.	Continuous mSCOA alignment and improvement.	Maintain	Medium	Maintain	Maintain	Maintain
12.	Continuous providing and monitoring of ongoing services. • Backups • Network • Firewall	Maintain	Medium	Maintain	Maintain	Maintain
13.	Functionality review on Samras financial system.	New	Medium	New Tender	Maintain	Maintain
14.	Business Continuity (Availability of ICT Network and systems)	Maintain	High	Maintain	Maintain	Maintain
15.	Upgrade Municipal Website	New	High	Tender for new Website	Maintain	Maintain
16.	Identified a new server room in Swellendam for ICT servers.	New	High	Maintain	Maintain	Maintain
17.	Procure new servers for ICT room and to implement disaster site	New	High	Maintain	Maintain	Maintain
18.	Develop intranet for municipality	New	Medium	Implement	Maintain	Maintain

Nr	Activity	Type of Project	Risk	Year 1 2026/2027	Year 2 2028/2029	Year 3 2029/2030
19.	Improve security controls: • Deactivate USB Ports • Block unauthorised downloads and Web sites • Enable MFA and SSPR	New	Medium	Implement	Maintain	Maintain
20.	Control all 3rd Party Systems/Applications in the Municipality	New	High	Implement	Maintain	Maintain
21.	ICT Smart City Concept • Integration of systems and apps • Job card system/tablets	New	Medium	Implement	Maintain	Maintain
22.	Implement ICT cyber awareness Sessions	New	Medium	Implement	Maintain	Maintain
23.	In-house ICT training on MO365 Apps	New	Medium	Implement	Maintain	Maintain

11) REVIEW

The content of the ICT Strategic Plan will be reviewed by the ICT Steering Committee and approved by Council as and when required, to reflect the current stance on ICT within the Swellendam Municipality.

+27 28 514 8500
info@swellenmun.co.za
swellenmun
www.swellenmun.co.za
+27 28 514 2694
49 Voortrek Street, Swellendam | P.O Box 20, Swellendam 6740

ICT STANDARD OPERATING PROSEDURE - USERS			Document Nr: SOP-ICT 01
Version: 1.0	**Effective Date: 1 July 2026**	**Review Date: 01/04/2026**	**Page: 1 - 17**
Compiled by:	ICT System Administrator	Name: A Meyer	**Signature:**
Approved by:	Director Financial Services	Name: E Wassermann	**Signature:**

1. ACCESS AND USE

1.1 As required the Municipality will provide remote access to users on the approval of the ICT MANAGER and Director Financial Service.

1.2 The Municipality will consider and authorise staff/vendors/providers as needed should require connecting through the remote access connection/VPN as needed.

1.3 If problems occur on a remote computer connection, it is the responsibility of the user to bring the laptop/device into the ICT section for the problem to be analysed there, unless the problem can be resolved remotely or virtually or any other way.

1.4 The Municipality will accept no responsibility for any damage done to the computer or information stored, either during transit or when being worked on. Staff and personnel are expected to employ proper due diligence, care, security and safety of the Municipality's assets removed from the premises.

1.5 Users may only access the Municipality's computer system, e-mail, and internet facilities by means of their own authorised usernames and passwords. The only variance would be where a unique situation exists which justifies a different handling which is brought to the attention of the ICT MANAGER and has received approval.

1.6 Apart from the ICT MANAGER and authorised ICT service provider, users shall not use any other username or passwords other than their own Municipal user details.

1.7 Users shall not knowingly allow the use of their username and/or password by anyone else and users are alerted to the fact that they are responsible for all work saved or retrieved, messages/documents/files sent or received, or transactions carried out via the internet and e-mail/system under their username and password.

1.8 Unauthorised users shall not access, copy, alter or delete the files or data of any other user.

1.9 Users shall not access or attempt to access networks resources or network drives in respect of which the user has no legitimate reason to access.

1.10 All users require the approval from the relevant Director and ICT MANAGER to access the municipality's Local Area Network/Wide Area Network and Other Information Network Resources.

1.11 If a person is transferred or fills another person's post (even in an acting capacity), no change will be affected by the ICT section until the HR department requests it.

1.12 When a person leaves the employ of the Municipality, it is the responsibility of the HR department to inform the ICT section to make the relevant changes and/or terminations.

1.13 Where a person is dismissed or suspended, the HR department is responsible for ensuring that the ICT section is informed without delay, so that the relevant access can be suspended, unless an alternative arrangement or request was considered and approved by the relevant Director in conjunction with the ICT MANAGER.

1.14 Usage of flash drives / memory sticks are discouraged to be used on Municipality equipment unless permission and approval is obtained from the relevant Director and ICT MANAGER. The reason for the prior approval is because traditionally; these devices pose the biggest threat for spreading viruses/malware.

2. PASSWORDS

To prevent the unauthorised access of the Municipality's computer system, passwords should comply with the following standards:

2.1 Passwords are personal and must not be disclosed or revealed to others.

2.2 Passwords should not be printed or stored online in any electronic form which can potentially be accessed by unauthorised individuals or persons.

2.3 Passwords must never be written down on a piece of paper or shared with anyone. Passwords must be kept safe and secret.

2.4 Use of passwords that can be guessed easily should be avoided.

2.5 Use different passwords for all user accounts.

2.6 No official is allowed to show or share their passwords with any work colleague or the ICT Service Division for any reason.

2.7 Passwords must not contain the user's "Account Name" or "Full Name". Both checks are not case sensitive.

2.8 Passwords must contain characters from three of the following five categories:

2.8.1 Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)

2.8.2 Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)

2.8.3 Base 10 digits (0 through 9)

2.8.4 Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

2.8.5 Non alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

2.9 Passwords should be changed every 30 days.

3. BACK-UPS

3.1 Should the ICT section need to remove a user's computer (for repairs, to reallocate etc.), a backup will be made of the data on the devise if possible.

3.2 Any information saved by the user on the user device desktop functionality will not be backup and safeguarded. The ICT section is not responsible for any loss and cannot assure recovery of any such data that may been lost.

3.3 All messages/files/documents on the e-mail server will be backed up regularly per the backup policy.

3.4 All files save under my documents will be backed up regularly per the backup policy.

3.5 If users require a more secretive (but not necessarily secure) method of storing data, they may place a password on each file. However, should the password be lost, be aware that no-one may be able to recover the file.

3.6 Employees should not make use of municipal owned storage space (i.e. servers, local hard drives, CD's, DVD's, memory sticks/flash drives/USB sticks, MP3 Players, external hard drives, or any other removable media) for storing any of the following content:

3.6.1 Private digital photos, documents and sketches;
3.6.2 Music files;
3.6.3 Movie clips or full-length movies;
3.6.4 Presentations and slide shows of entertainment nature.

3.7 The determination of the extent of the above misuse being acceptable or not; would lie with the assessment of the ICT MANAGER if unclear.

4. SECURITY

Physical Security

4.1 It is the responsibility of every user to ensure that their computer and associated peripheral devices are adequately protected/secured against theft and damage.

4.2 In the case of a desktop computer and peripherals, the user should ensure that the office in which the desktop computer is resident is adequately secured at the close of business, or whilst unattended for any lengthy period by locking their office as best possible.

4.3 In the case of a laptop computer, and the device is not taken home, the user should ensure the laptop is lock away in a safe place before leaving the office, the building and office doors are locked and the alarm security systems are activated.

4.4 It is the users' responsibility to ensure that their equipment is protected against misuse.

4.5 If you take any devices home, ensure that your labtop is in a safe location, doors are locked in the event of you leaving your premises; and activate your home security system if you have one installed.

4.6 If you are staying in a hotel, lock these devices in a safe when you leave your room.

4.7 Keep these devices in your sight when passing airport checkpoints.

4.8 If you travel by car, lock these devices in the trunk when you leave your car.

4.9 Refrain from using these devices in locations that might increase the likelihood of damage and/or loss/theft.

4.10 Keep food and beverages away from these devices to prevent accidents and damage.

4.11 Use a padded carrying case for these devices if available.

Logical Security

4.12 Users are responsible for ensuring the security, integrity and confidentiality of all data and information resident on their personal computers.

4.13 In addition to the rules relating to passwords, users shall take reasonable steps to ensure that no confidential information resident in their personal computer is:

4.13.1 Visible during their absence from their PC.
4.13.2 Accessible by unauthorised persons.

4.14 Reasonable steps shall include:

4.14.1 Systems that are kept on, are signed off to a "login/locked" state for security purposes. Where unique circumstances exist to vary from this recommendation, the request to soften this requirement must be made to and approved by relevant Director in conjunction with the ICT MANAGER.
4.14.2 Requiring passwords to open files containing confidential information.

Saving and Removal of Data

4.15 Users are strictly prohibited from saving Municipality data, confidential information or files onto disk, CD-ROM or any electronic or other storage media and removing them from the Municipality's premises without permission.

4.16 A user requiring access to Municipality data, confidential information, or files whilst in any location other than at the Municipality premises, shall obtain the express permission at the Municipal Manager office, through the POPIA application form and approval.

4.17 The remote use of Municipality data, confidential information or files may only be used by users and authorised individuals/companies in the performance of their work functions through a secure VPN Access.

4.18 Municipality's data, confidential information or files will remain the property of the Municipality.

4.19 As and when possible, the user further undertakes to protect and safeguard the data, information and files in a diligent and conscientious manner, and to perform a comprehensive virus/malware scan where the data or information has been used on a personal computer or other device not belonging to the Municipality, prior to reintroducing data or information onto a Municipality PC, network or any municipal computer system.

5. MAINTENANCE AND FAULTS

Computer System Maintenance

5.1 Only the correct authorised technical staff from the ICT Section and ICT Service provider shall carry out maintenance and support of the Municipality computer system and peripherals. Accordingly, users may under no circumstances:

5.1.1 Attempt to repair the PC in their use, or those of other users.

5.1.2 Allow an unauthorised technician to perform any support, repair, or maintenance on the Municipality computer system.

Faults

5.2 If users have ICT, software problems or faulty equipment, then the following procedures must be followed:

5.3 Report all ICT problems to the ICT section (Ext 449) or via email on itsupport@swellendam.gov.za .A job card/ticket will be issued to an available technician, and the problem will be seen to as soon as possible. A ticket/reference number will be provided to the user which they can use to follow up on progress of their reported issue.

5.4 To assist timeously, the ICT section may require remote access to a user's machine to resolve the problem.

5.5 In the case of faulty equipment which cannot be repaired on site, the ICT System Administrator or service provider will evaluate and assess the extent of the fault and to determine whether the equipment should be repaired or replaced.

5.6 All ICT equipment must be procured by the ICT section. Special request items will require motivation and approval between the relevant Director and ICT MANAGER.

5.7 If there is no equipment available to replace faulty hardware, an alternative or temporary solution may be made available as possible.

6. SOFTWARE

6.1 The Municipality has licensed, procured or developed software for use on the Municipality computer systems. This software is proprietary to Municipality.

6.2 Swellendam Municipality and its employees are legally bound to comply with the Copyright Act 8 of 1978 and all proprietary software license agreements.

6.3 Non-compliance can expose Swellendam Municipality and the responsible employee(s) to civil and/or criminal penalties.

6.4 To protect its proprietary interests and to ensure compliance with the terms of applicable licenses, users are expressly prohibited to install any software onto his or her computer.

6.5 All installation must be done by the ICT section, this includes the downloading of any program files from the Internet.

6.6 If at any stage a user believes that a software product, whether freeware, shareware, or proprietary software, would assist in the furtherance of the Municipality's business then a motivation should be sent to the relevant Director and ICT MANAGER for approval and consideration.

6.7 Modifying, revising or adapting any Municipality software is prohibited.

6.8 All new software must be tested, reviewed and approved by the ICT section prior to deployment on municipal equipment.

6.9 Altering, or attempting to alter, yours or any others user's system configuration is prohibited.

6.10 Should employee receive a CD or a disk that provides a demo of software or any other item, it must be presented to the ICT section first, which will install them correctly for the user, and uninstall it if practical when the usage has expired.

6.11 The ICT section may refuse to install any software should they believe that is not appropriate for the Municipality's ICT systems or creates any problems or risk for the Municipality.

6.12 The ICT section will in conjunction with the relevant directorate as far as possible provide appropriate software for staff members per their job requirements.

6.13 No person may copy, load, or run any software that is not properly legally licensed.

7. HARDWARE

7.1 Personnel will contact the ICT MANAGER with a computer hardware need, including information from the department on the purpose and use of the computer hardware.

7.2 The ICT MANAGER will assist with the establishment of the specifications of required ICT equipment/specification based on the request and operational function to be performed as best practically possible within their ability and expertise.

7.3 Procurement of all ICT equipment is completed by the ICT MANAGER after approval by the Director Financial Services.

7.4 The ICT department may arrange or facilitate installation and configuration of all computer hardware as best possible or may make a suitable arrangement to do so in conjunction with the relevant department or service provider.

7.5 Outside equipment should not be connected to the Municipality's network without the ICT MANAGER's permission.

7.6 No unauthorised person may open a computer/device or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by a competent person from or provided by the ICT section.

7.7 All municipal ICT equipment remains the property of the Municipality and must be returned to the ICT section when an employee leaves the Municipality.

8. PRINTERS

8.1 All users that require printing facilities will have access to a printer as far as practically possible under the relevant circumstances.

8.2 All special purpose printing requirements must be discussed with the ICT MANAGER for consideration and approval.

8.3 No unauthorised and unqualified person may open a printer or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by the ICT section, or a competent provider arranged in conjunction with ICT. The only exception is to replace an ink cartridge or correcting paper jams, which may be carried out by the user only if they are sufficiently skilled and abled to do so without causing any damage.

8.4 Network printers will be made available to staff within proximity and may not be based on departmental, building or directorate boundaries.

8.5 The Municipality will provide ink and toner cartridges for officially approved and procured printers only.

8.6 If any damage occurs to a printer, the user needs to notify the ICT helpdesk as soon as possible to assist.

8.7 Users must refrain from printing multiple copies of the same document and make all attempts to reduce printing.

8.8 Users are to try to limit paper usage by taking advantage of duplex printing (i.e. double sided printing) features offered by some printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page). If they are uncertain how to do this, they are welcome to contact the ICT section for assistance.

8.9 Avoid printing large files, as this puts a strain on network resources and interferes with the ability of others to use the printer.

8.10 Avoid printing e-mail messages. This is wasteful. Instead, use the folders and adobe printing to safe the emails to your my document folder.

8.11 Use the print preview option instead of printing a document to see what it looks like. This is a less wasteful alternative.

8.12 Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with the ICT section first.

8.13 Colour printing is typically not required by general business users. Given the selective need, as well as the high cost per page to print colour copies, colour printers and printing are to be minimized.

8.14 Replacement of Toners relating to the photocopiers will be the responsibility of the relevant service provider/s concerned.

8.15 At all costs please do not print documents unnecessarily or create manual paper-based procedures and systems. Digital and automated systems are preferred as it saves costs, is faster and safer when using centralized or cloud storage, servers, and systems. If uncertain about any of this, please feel free to contact the ICT section for advice.

9. VIRUS/MALWARE PROTECTION

9.1 Users are alerted to the fact that viruses and malware can cause substantial harm to the Municipality's computer systems, networks, data, reputation, and cost money. The damage caused is often not limited to hardware or software but can result in further losses to the Municipality because of lost production, man hours, maintenance, and recovery of work.

9.2 The ICT MANAGER is to ensure that as best possible the latest approved antivirus/malware protection software has been installed on the PC/Laptop, that it is permanently enabled and that the newest signature update is available as best practical and possible.

9.3 Should any data be received by a user via disk; CD-ROM, flash drive, USB, internet, email or any other source, a comprehensive scan of that data should be performed prior to loading that data to the computer system or network of Municipality.

9.4 However, it remains the responsibility of the user to make sure that their antivirus/malware/Windows/store packages are up to date and if not, to contact the ICT section immediately for assistance.

9.5 If a virus/malware is detected, it must be reported immediately to the ICT System Administrator.

9.6 Be aware of suspicions mails to reset passwords or files send with a link. If unsure if the mail is safe, kindly contact the ICT System Administrator. Before opening the email ensure that you know the person who send it by checking the email address.

9.7 Suspicious emails are normally sent from, Gmail, Yahoo, etc of which an example is: "Elmari Wassermann dr.zetiaziz@mail.com"

10. INTERNET USAGE

10.1 Users granted internet access via the Municipality computer system are required to apply for it by obtaining the approval of their relevant Director/ICT MANAGER and forward it to the ICT section for activation. Due to the nature of the internet, it is essential that users comply with the following rules. Failure to do so could have serious economic, financial and security consequences for the Municipality and may result in the personal liability and disciplinary steps against the User:

10.1.1 Users may not use Municipality Internet/Wi-Fi access to conduct any other business than that of the Municipality except as otherwise authorised by the relevant Director/ICT MANAGER. The determination of the prior if unclear resides with the ICT MANAGER.

10.1.2 Users may not use Municipality Internet access to host or display personal web pages.

10.1.3 User's internet access / usage can be monitored without prior notification if Swellendam Municipality deems this necessary. If there is evidence that a user is not adhering to the guidelines set out in this policy, Swellendam Municipality reserves the right to investigate and take disciplinary action, including termination and/or legal action.

10.1.4 Users using the Internet are representing Swellendam Municipality. Users are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner.

10.1.5 Users must not use the Internet for purposes that is illegal, unethical, non-productive or harmful to Swellendam Municipality.

10.1.6 No user shall use a computer to access or download any inappropriate item, which may - inter alia - include:

a) Any item which carries any defamatory, discriminatory or obscene material.

b) Any item which carries any sexually explicit message, images, cartoons or jokes.
c) Any item which contain religious, racist or sexist slurs.
d) Any item which may be seen to be insulting, disruptive, and offensive to other people.

10.1.7 Users may not browse or download any documents or images not related to Municipality business read in the context of 10.1.1 above.

10.1.8 Users may not subscribe to or participate in Chat Groups, Bulletin Boards, Newsgroups, or discussion groups that are not work related and have not been approved in advance by the relevant Director and ICT MANAGER.

10.1.9 Unless specifically authorised/delegated/approved otherwise, Users may not transact on behalf of the Municipality via the Internet (i.e. purchase of goods or services).

10.1.10 Downloading of data via File Transfer Protocol (FTP) Websites is permitted if it is work related for which the ICT section can be contacted for assistance.

10.1.11 Users are strictly prohibited from posting sensitive information such as usernames, passwords, security codes or server/network-specific information which could assist third parties wishing to gain unauthorised access to the Municipality computer system.

10.1.12 Users are prohibited from publishing or transmitting confidential information on or via the Internet. If a situation exists where prohibited/confidential information must be transmitted, approval will be required from the relevant Director/ICT MANAGER prior to the transmission or publication of such information on or via the Internet.

10.1.13 Users may not knowingly introduce viruses/malware or any risky items into the Municipality computer system and networks.

10.1.14 Subscriptions to online services are limited only to services that will enhance and promote the business of the Municipality and subject to the relevant Director in conjunction with the ICT MANAGER for approval.

10.1.15 Electronic Banking and other such reasonable personal services are permitted to all users within reason, but the Municipality will not be held liable for any activities pertaining to these services.

10.1.16 This privilege regarding personal services may be revoked if it found that its use is impacting negatively on the performance of the employee or Municipality in any way, form, or cost.

10.1.17 Anyone seen abusing the internet, must be reported to the Director and ICT MANAGER.

11. E-MAIL USAGE

11.1 E-mail is a business communication tool and users are obliged to use this tool in a responsible, effective, and lawful/correct manner.

11.2 The Municipality e-mail system may not be used:

11.2.1 To initiate or forward any chain-message or other message which asks the recipient to forward such message to multiple other users unless required for work purposes;
11.2.2 To send frequent unsolicited Commercial/spam e-mail to persons with whom the sender does not have a prior relationship.
11.2.3 To send frequent and/or numerous e-mail messages with the intention of disrupting or inconveniencing the receiver;

11.3 The use of the Municipality e-mail facilities to send, download, display or store prohibited material is strictly prohibited.

11.4 No user may use email to send any inappropriate items, which may - inter alia - include:

11.4.1 Any item which carries any defamatory, discriminatory or obscene material.
11.4.2 Any item which carries any sexually explicit message, images, cartoons or jokes.
11.4.3 Any item which contains religious, racist or sexist slurs.
11.4.4 Any item which may be seen to be insulting, disruptive, and offensive to other people.

11.5 No employee shall knowingly receive or store e-mail or any form of electronic communication containing prohibited material.

11.6 If any employee is uncertain as to whether any material or statement constitutes prohibited material, such employee must obtain clarification from the relevant Director in conjunction with the ICT MANAGER without delay.

11.7 E-mail containing prohibited material which has been inadvertently received shall be deleted by the employee receiving such e-mail, immediately that he or she becomes aware of the content thereof and the incident must be reported to the relevant Director and the ICT MANAGER without delay.

11.8 Although by its nature e-mail seems to be less formal than other written communication, the same laws apply, and therefore must follow the communication policy of Swellendam Municipality. Approvals and electronic/digital signatures via email carry the same weight as a physical documented approval or signature.

11.9 No users may send e-mail messages using another person's e-mail account unless specifically authorised or requested to do so with valid cause and reason.

11.10 All users are expected to read their e-mail and process/update their Collaborator document management system and performance management system regularly.

11.11 E-mail messages are written business records and are subject to Swellendam Municipality's rules and policies for retaining and deleting business records.

11.12 You must have no expectation of privacy in anything you create, send or receive on the Municipality's computer system. Your e-mails/documents/files can be monitored without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, Swellendam Municipality reserves the right to take disciplinary action, including termination and/or legal action.

11.13 All e-mail accounts and emails created/maintained on the Municipality's e-mail system remain the property of Swellendam Municipality.

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

11.15 All users are expected to undertake regular housekeeping of their e-mail systems and device on a regular basis. This involves deleting or archiving (as appropriate) messages/files that are no longer required. All attachments which need to be kept should be saved to disk, archived, and the e-mails/files deleted where practical. Users are also required to empty the "Deleted items" folder on a regular basis.

11.16 The e-mail system is ideally not a system to archive important information or messages; this should be saved to the relevant disks or network drives. The ICT section will not take responsibility for lost / archived or missing email messages or files.

11.17 No spamming is allowed.

11.18 Users may not to disguise their identity while using Municipality systems.

11.19 Users may not alter or manipulate the "From" line or any other indication of the origin of an e-mail message.

11.20 When communicating to many recipients, especially external of the municipality, the email addresses must be placed in the "Bcc" section of the email. This is to protect email addresses from spammers.

11.21 E-mail signatures must be aligned to the Swellendam Municipality corporate identity manual and must not contain personal slogans or sayings. The Municipality corporate identity and branding guidelines held by the Communications department always retain preference in this regard.

E-Mail personal use

11.22 Although Swellendam Municipality's e-mail system is meant for business use, Swellendam Municipality allows use of e-mail for personal use if certain guidelines are adhered to:

- 11.22.1 Personal use of e-mail should not interfere with work.
- 11.22.2 Personal e-mails must also adhere to the guidelines in this policy.
- 11.22.3 The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
- 11.22.4 No mass or chain mailings, i.e. messages containing instructions to forward the message to others.
- 11.22.5 All messages distributed via the Municipality's e-mail system, even personal e-mails, are Swellendam Municipality's property.

Legal risks of e-mail

11.23 If you send or forward e-mails with any libelous, defamatory, offensive, racist or obscene remarks, you and Swellendam Municipality can be held liable.

11.24 If you unlawfully forward confidential information, you and Swellendam Municipality can be held liable.

11.25 If you unlawfully forward or copy messages without permission, you and Swellendam Municipality can be held liable for copyright infringement.

11.26 If you send an email/attachment that contains a virus/malware, you and Swellendam Municipality can be held liable.

12. MONITORING, ACCESS TO AND DISCLOSURE OF E-MAIL AND INTERNET USE

Monitoring

12.1 The Municipality computer system is provided to employees, at Municipality expense, for the employees' use for Municipality business. To protect its rights and interests, the Municipality can procure software monitoring applications, which may assist with routinely monitoring all Internet/device/hardware/software usage and e-mail/file traffic on the Municipality e-mail and related system.

12.2 Thus, whilst all e-mail/work will not be routinely read/checked, any e-mails/files identified as potentially infringing any policy may be accessed, reviewed, and read by the ICT MANAGER or his/her alternate. The Municipality reserves the right to access and read the contents of e-mail messages/files/documents and track/assess usage in the following circumstances:

12.2.1 Insofar as it is required by law or by legal obligations to third parties to do so,
12.2.2 If it has a legitimate business need or reason to do so,
12.2.3 To protect its interests if it reasonably suspects that an employee has committed or is committing a crime that might be aimed at or attributable to the Municipality,
12.2.4 If it is of the bona fide opinion that such access or disclosure may be necessary to investigate a breach of the security of the e-mail system or of this policy or disciplinary policy.

12.3 Should the ICT MANAGER or his/her alternate encounter indications of illegal/unacceptable activity or violations of Municipality policy or security, the ICT MANAGER or his/her alternate shall investigate further and report any finding to the relevant Director/Municipal Manager.

12.4 Employees must ensure that all business-related e-mail messages/files/documents that should be available to other employees of the Municipality remain available.

The employee consents to access by the Municipality to protect system security or The Municipality's proprietary rights.

Unauthorised use to be reported.

12.5 Users shall not knowingly permit/allow the unauthorised use of the Municipality's e-mail and related network/system. Any unauthorised use of the Municipality's e-mail/related systems must be reported without delay to the relevant Director/Municipal Manager in which the unauthorised use occurred, and to the ICT MANAGER without delay.