

**MANAGING ELECTRONIC RECORDS IN
DRAKENSTEIN MUNICIPALITY**

Content

1. INTRODUCTION	2
1.1 Statutory and regulatory framework	2
1.2 Relation to other information and communication technology policies.	3
2. WHAT IS AN ELECTRONIC RECORD?	3
3. MANAGEMENT OF ELECTRONIC RECORDS AND RESPONSIBILITIES.....	3
3.1. Schedule of electronic records.....	3
3.2 Appraisal and disposal	3
3.2.1 Transfer	3
3.2.2 Destruction	4
3.3 Accessibility	5
3.3.1 File formats.....	4
3.3.2 Storage media.....	5
3.3.3 Migration	5
3.4 Metadata	5
3.4.1 Roles & Responsibilities.....	6
3.5 Authenticity	6
3.5.1 Audit and history trail	6
3.6 Back-up and disaster recovery.....	7
4. MANAGEMENT OF RECORDS MAINTAINED ON INDIVIDUAL PC'S AND NETWORK DRIVES.....	8
5. MANAGEMENT OF RECORDS IN IMAGING AND SCANNING SYSTEMS.....	8
6. MANAGEMENT OF WEBSITES AND WEB BASED ACTIVITIES AS RECORDS.....	8

ANNEXURES

Annexure “A” - Application for Approval of Electronic System

APPROVED/AMENDED

MEETING

DATE

APPROVED

Council

24/11/2010

1. INTRODUCTION

Records are the output of the business and administrative processes of Drakenstein Municipality. In other words, the final proof that a business or administrative process was transacted. It serves as essential proof of the business that was conducted and should remain unaltered over time for as long as they are needed.

The need for effective management of records is enhanced by the Public Finance Management Act, 1999, the Promotion of Access to Information Act, 2000, the Promotion of Administrative Justice Act, 2000, and the Electronic Communications and Transactions Act, 2000 in terms of which the municipality has an obligation to manage its records properly, to provide access to information contained in records, to provide reasons for administrative decisions and to ensure the authenticity of records.

In order to meet its record keeping responsibilities, and to adhere to paragraph 11.1.2 of its Records Management Policy, Drakenstein Municipality hereby determines the under mentioned guidelines and principles as its policy to ensure that electronic records are accessible and readable over time in terms of an active programme committed to managing and preserving records from their creation to final disposal.

1.1 Statutory and regulatory framework

In terms of the National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended and the Regulations published in terms of the act, the Records Manager shall be responsible for ensuring that all records of such body -

- (a) receive appropriate physical care;
- (b) are protected by appropriate security measures; and
- (c) are managed in terms of standing orders of the municipality and other

relevant legislation.

With reference to the electronic records of the municipality, the following Act is of particular importance:

1.1.1 The Electronic Communications and Transactions Act (Act. No. 25 of 2002)

The purpose of the Act is to legalise electronic communications and transactions, and to build trust in electronic records. According to the Electronic Communications and Transactions Act data messages are legally admissible records, provided that their authenticity and reliability as true evidence of a transaction can be proven beyond any doubt.

The evidential weight of electronic records (including e-mails) depends amongst others on the reliability of the manner in which the originator and the receiver managed the messages. Should the municipality not have a properly enforced records management and e-mail policy and a reliable and secure record keeping system, it runs the risk that the evidential weight of its electronic records (including e-mails) is being diminished.

1.2 Relation to other information and communication technology policies

This policy document must be read with the existing information and communication technology policy (computer policy) of the municipality which is contained in the document attached as **ANNEXURE A** hereto.

2. WHAT IS AN ELECTRONIC RECORD?

Electronic records mean information which is generated electronically and stored by means of computer technology, while an **electronic records system** is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and metadata (descriptive, background and technical information regarding the information stored electronically.)

Electronic records can either exist in structured applications, which hold transactional records (i.e. Collaborator, Venus, etc.) or in unstructured applications (i.e. electronic records generated on individual PC's and in e-mail systems).

3. MANAGEMENT OF ELECTRONIC RECORDS AND RESPONSIBILITIES

In view of the specialised nature of electronic records, all responsibilities attributed to the Records Manager in this policy document must be read to include the words: ***“in collaboration with the Information and Communication Technology Manager.”***

The **“responsible person”** referred to in this document means the person responsible for the installation and operation of any electronic system in terms of which electronic records or data is generated and includes any supplier of electronic systems and an operator of any system within the municipality in terms of a service level agreement.

In order to classify and appraise electronic records as contemplated in paragraph 3.2 below, the Records Manager must compile a comprehensive inventory of all the electronic records systems containing a brief description of the purpose of each system in the following format:

Name of System	Purpose of system	Functions
CTRACK Responsible Person:	To keep track of all municipal vehicles	<ul style="list-style-type: none">• Monitoring movement;• Monitoring usage, etc;

3.1 Schedule of electronic records systems

In order to ensure that all electronic record systems are included in the inventory referred to in 3 above, department heads must notify the Records Manager in writing of all systems in use in their various departments.

¹ *National Archives “Managing Electronic Records in Governmental Bodies: Policy, Principles and Requirements.”*

No new systems may be implemented in any department or section of the municipality without prior approval of the ICT Steering Committee. Application for approval must be submitted to the said committee on an application form as per example attached as **Annexure A**.

The management of all electronic records generated by the municipality will be the responsibility of the Records Manager. The management of these records will be undertaken within the frameworks and guidelines provided by the National Archives as contemplated in the Municipality's Records Management Policy.

The responsible person, with the assistance of the ICT Manager, must ensure integrity of the records by capturing them at creation into record keeping systems that-

- 3.1.1 routinely capture all records;
- 3.1.2 organises captured records in a way that reflects the functions of the municipality;
- 3.1.3 protect the records from alteration or unauthorised disposal; and
- 3.1.4 provide access to the information kept.

3.2 Appraisal and disposal

The Records Manager must ensure that all electronic records are included in and dealt with in terms of the Schedule of Electronic Records Systems and ensure that disposal instructions and procedures in respect thereof be obtained in collaboration with the National Archives and Records Service on a regular basis.

3.2.1 Transfer

The Records Manager shall be responsible to identify which records have long-term archival value and should be preserved as part of the national archival heritage. Such records have to be transferred into archival custody.

To ensure that the authenticity of records can be proven after they have been transferred, the Records Manager must establish the following controls over the transfer that would demonstrate an unbroken chain of custody-

- 3.2.1.1 establishing procedures for registering the records' export;
- 3.2.1.2 examining the records to determine whether they correspond to the records that are designated in the disposal authority governing their export; and
- 3.2.1.3 formally importing the records on to the new platform.

The Records Manager must assess and verify the authenticity of the creator's records. This includes verifying that the metadata and audit trail data relating to the identity and integrity of the records have been carried forward with them along with any relevant documentation.

3.2.2 Destruction

The Records Manager must ensure that destruction of records is carried out in terms of a documented process and subject to the provisions of paragraph 8 of the municipality's Records Management Policy, the Records Manager must –

- 3.2.2.1 ensure that no records be destroyed without a written disposal authority being issued;

- 3.2.2.2 obtain a disposal authority from the National Archives and Records Service and keep it on record;
- 3.2.2.3 determine retention periods and document the reasons behind the retention periods;
- 3.2.2.4 document when and how destruction should be carried out;
- 3.2.2.5 document the names of officials responsible for authorising destruction processes;
- 3.2.2.6 ensure that destruction certificates are compiled and kept on record; and
- 3.2.2.7 document destruction actions in audit trail data.

3.3 Accessibility

As new releases of software do not necessarily enable access to older formats, records generated in obsolete formats may become inaccessible. The Records Manager must therefore ensure that the records themselves are adapted or migrated regularly to be compatible with the new formats, storage media and systems as technological change takes place. In this regard the Records Manager will pay specific attention to the following-

3.3.1 File formats

Since format is fundamental to all accessibility and preservation actions, the responsible person must ensure that the risk of format obsolescence is managed timeously. In doing so the responsible person in collaboration with the ICT Manager must provide the Records Manager and the relevant head of department with timely notification that formats are in danger of becoming obsolete and with a suggested format migration path with the view to ensure that the information to be migrated will remain accessible.

Regular consultation with the manufacturers/developers of software or data management systems must be undertaken by the responsible person to determine the safest options for file formats, i.e. PDF or any other format recommended. Feedback of such consultation must be given to the ICT Manager.

3.3.2 Storage media

Should it be necessary to archive, the Records Manager must ensure that the storage media for electronic records can be read in order to access such records. He/she must determine special requirements for the preservation of records that have to be preserved indefinitely. In doing so he/she must ensure that the records are preserved in a manner that safeguards it against environmental factors such as extreme temperatures, humidity, oxidation, dust and magnetic fields.

In order to continuously monitor whether the storage media on which records are held are in danger of becoming obsolete, and to monitor whether the storage media in their custody are degrading, the following media watch strategy will apply-

The responsible person, in collaboration with suppliers where applicable, must provide the Records Manager with continuous notification that-

- 3.3.2.1 storage media is in danger of becoming obsolete;
- 3.3.2.2 data is degrading; and
- 3.3.2.3 media is degrading.

In support of 3.3.2.1 and 3.3.2.3 the responsible person, in collaboration with suppliers where applicable, must undertake timely maintenance and migration actions to prevent records from becoming inaccessible.

3.3.3 Migration

Since electronic records need to be migrated to new hardware and software platforms constantly to enable them to remain accessible, the following strategy to preserve their integrity and to retain their accessibility shall apply:

The ICT Manager, in collaboration with the responsible person and suppliers/developers of electronic records systems shall-

- 3.3.3.1 determine specific options for migration and how they will be used;
- 3.3.3.2 assign responsibility for migration to a specific person or unit;
- 3.3.3.3 assess the impact of this migration strategy on the integrity and utility of records;
and
- 3.3.3.4 implement an appropriate quality control procedure for migration;

3.4 Metadata

According to SANS 15489 metadata is “data describing the context, content and structure of records and their management through time.” In short, descriptive metadata gives information about where a record comes from, who the creator was, when it was created, where it is located, etc.

Therefore metadata itself also needs to be managed, to ensure that they are unalterable and thus trustworthy and reliable. It follows that only creators/users with the necessary authorisation have access to the metadata database to allow for documented and auditable changes to be done when necessary.

3.4.1 Roles and responsibilities

- 3.4.1.1 Although the overall responsibility for the management of electronic records rests with the Records Manager, the relevant executive directors, heads of departments and responsible persons have a duty to notify the Records Manager in writing of any application in terms of paragraph 3.1 to acquire new electronic systems or changes in existing systems.
- 3.4.1.2 The Responsible person, in conjunction with suppliers and the relevant head of department, will be responsible for the capturing and management of records metadata throughout the life-cycle of the record and to develop related policies and strategies, and monitor the process of metadata creation. He/she will also be responsible for the training of users on capturing, managing and using metadata.
- 3.4.1.3 All employees are responsible and accountable for ensuring the accuracy and completeness of the records management metadata for which they are responsible.
- 3.4.1.4 Heads of departments must ensure that internal controls are in place so that customers, auditors, courts, and other authorised users can rely on the information that the municipality produces.
- 3.4.1.5 The Responsible person must ensure the reliability, usability and integrity of the systems used to capture and maintain metadata. They are responsible for ensuring that all records management metadata is linked to the related records and that these links are maintained.

3.4.1.6 If multiple copies of the same record exist, the responsible person must establish procedures that would identify the authoritative record, to ensure that it is protected and preserved.

3.4.1.7 The relevant Executive Directors are responsible to ensure that the activities in paragraphs 3.4.1.1 to 3.4.1.5 are executed.

3.5 Authenticity

Information contained in records is a means of ensuring accountability and it may need to be produced as evidence in courts of law. Section 15 of the Electronic Communications and Transactions Act provides for legal recognition of electronic evidence, but only in so far as the integrity, authenticity and reliability of the evidence can be proven.

The Records Manager must ensure that suppliers or developers of electronic records systems must certify and confirm the authenticity, reliability, integrity, accuracy, adequacy and completeness of records generated by such systems and the measures to protect such records against alterations by users and system administrators.

3.5.1 Audit and history trail

Depending upon the application and the system, as well as on the specific needs of the municipality, the ICT Manager must determine which audit trail data is critical to prove authenticity and must then document the types of audit trail data to be captured, as well as the process whereby the audit trail will be captured.

Since audit trail data is fundamental to prove the authenticity of records, the Records Manager must describe-

3.5.1.1 who may access such records and for what purposes;

3.5.1.2 the procedures for such access;

3.5.1.3 how to interpret the data; and

3.5.1.4 the migration of audit trail data from one storage medium to another.

3.6 Back-up and system recovery

The purpose of a back-up and system recovery procedure is to rebuild authentic and reliable records. The ICT Manager must therefore ensure that the existing backup strategy of the municipality addresses the following:

3.6.1 that back-up data include the associated metadata and audit trails of all records so that the authenticity of recovered records is not compromised;

3.6.2 the monitoring and auditing of the back-up data to verify reliability;

3.6.3 the storage of back-up data;

3.6.4 that the system technical manual contains sufficient information about the back-up data to ensure that it can be rebuilt and interpreted correctly; and

3.6.5 that procedures for checking that file integrity has not been compromised and that frequent testing of back-up media is undertaken to prevent data degradation.

4. MANAGING RECORDS MAINTAINED ON INDIVIDUAL PC,S AND NETWORK DRIVES

Each user must ensure that the records that are created on individual PC's are saved to a shared workspace on the municipality's network so that the information they contain can be

shared and re-used and that proper retention and disposal rules can be applied after a written disposal authority has been obtained from the National Archivist.

No official data may be saved on personal computers.

5. MANAGING RECORDS IN IMAGING AND SCANNING SYSTEMS

Even though the Electronic Communications and Transactions Act provides for electronic images to carry evidential weight, it only does so if it can be demonstrated that the records created in such systems were created in a trustworthy manner and there was no room to tamper with the records in the scanning process.

All personnel or users must ensure that all paper documents are examined prior to the scanning process, to ensure that a successful image is obtained. To ensure the suitability for scanning he/she must develop and document the procedures -

- 5.1 for such examination prior to the scanning process. Factors such as their physical state (thin paper, creased, stapled, etc.), and the attributes of the information (black-and-white, colour, tonal range, etc.) should be considered;
- 5.2 for documents which are found unlikely to be accepted by the scanner. For example, the original could be photocopied, or transparent wallets could be used; and
- 5.3 for scanning multi-page documents bound together with staples or clips.

When removing staples, clips or other document bindings, users must ensure that no damage is caused to the original that may affect the capture of the information from the document.

Where a source document has physical attachments, for example, stick-on notes, the system should provide facilities for distinguishing these from the document to which they are attached. Where there is a risk that an attachment might obscure, or be considered to obscure information on the source document, users must ensure that an image of the source document without the attachment is captured.

Where a source document has physical amendments, for example, white opaque paint, the system should ensure that the presence of such amendments is noted.

6. MANAGING WEBSITES AND WEB-BASED ACTIVITIES AS RECORDS

A website is a collection of information, records, or databases that is provided to a user community through a web interface. Web-based activities refer to the interactive communication of information and/or the conduct of business activities through web technologies.

The responsible person is responsible for the creation of authentic, reliable and accurate records of all web-based activities to enable them to be accountable to the public to which the services are provided.

The Records Manager is responsible for the management and preservation of records that may be generated through web based activities in accordance with the management principles as contemplated in paragraph 3 above.

ooo000ooo

ANNEXURE "A"

DRAKENSTEIN MUNICIPALITY

APPLICATION FOR APPROVAL OF ELECTRONIC SYSTEM

PART A: (To be completed by department applying for approval)

DEPARTMENT:.....

To:

- 1. **The Secretary
ICT Steering Committee;**

Application is hereby made for approval by your committee for the installation and operation of

.....
(Short description of the electronic system and motivation)

Full detail of the system is listed below.

.....
(Head of Department)

.....
(Date)

DETAIL INFORMATION OF ELECTRONIC SYSTEM(S)

- | | |
|--|---|
| 1. Name of system
.....
..... | Indicate the commonly used name and acronym of the system |
| 2. System control number
..... | Specify the internal control number assigned to the system for reference, control or cataloguing purposes, e.g. the information system's inventory number |
| 3. Municipal programmes supported by the system
.....
.....
..... | List programmes supported by the system |
| 4. Legislation or directives
.....
..... | Cite any laws or regulations authorizing or prescribing such programmes |

.....

5. Programme personnel

.....
.....
.....
.....

List the names and detail of the programme personnel who can provide additional information about the programme and the system supporting it. Such detail may include personnel of suppliers or outside providers of electronic records systems.

6. System purpose

.....
.
.....
.....
.....

Indicate the reasons for the system and the requirements met by it

7. Data input and sources

.....
.
.....
.
.....
.
.....
.

Describe the primary data input sources and the providers of data to the system. Plus detail of any other systems, inside or outside the municipality, from which the system receives data

8. Major output

.....
.....
.....
.....
.....
.....

8.1 Indicate the system's main products and the frequency of their preparation, e.g. reports, tables, charts, graphic displays, catalogues or correspondence – prepared weekly, monthly or annually.

8.2 Also indicate whether the information is transferred to other systems

9. Information content

.....
.....
.....
.....
.....
.....

9.1 Indicate the main subject matter, date coverage, time span, geographic coverage, update cycle and other major characteristics of the system.

9.2 Also indicate whether the system saves superseded information and whether it contains micro data or summary data

10. Location of documentation needed to read and understand the files

.....
. . .
.....
. . .
.....
. . .
.....
. . .
.....
. . .
.....
. . .
.....
. . .
.....
. . .
.....

10.1 Indicate where the code books and file layouts are maintained.

10.2 Indicate the office, room number and name of the custodian of the documents.

10.3 Indicate security and privacy as well as access restrictions.

- | | |
|------------------------|---|
| 11. Storage management | 11.1 Describe the storage media where master copies, backups and other copies will be kept. |
| | |
| | |
| | 11.2 Describe the storage environment in which the records will be kept |
| | |
| | 11.3 Describe how often records will be checked for deterioration |
| | |
| | 11.4 Describe the migration strategy for the records and how often migration to new technologies will be done |
| | |
| | |

PART B: (To be completed by the Chairperson of the ICT Steering Committee)

Application approved/refused (Give reasons for refusal if applicable)

(List conditions for approval if applicable)

.....
 (Chairperson: ICT Steering Committee)

.....
 (Date)

PART C: (To be completed by the Records Manager)

It is hereby certified that particulars of the electronic system herein approved has been noted in the Schedule of Electronic Records with the Disposal Instruction of

.....
 (Records Manager)

.....
 (Date)

