MUNISIPALITEIT
RICHTERSVELD
MUNICIPALITY

E-MAIL RECORDS MANAGEMENT POLICY FOR

RICHTERSVELD MUNICIPALITY

Version 1 of JULY 2019

Content

E-Mail Policy for Richtersveld Municipality

1. Purpose

1.1 The National Archives and Records Service Act applies to e-mail in the same way as it does to records that are created using any other media.

1.2 All public servants are required to create and preserve records of the Richtersveld Municipality's organization, functions, policies, decisions, procedures and transactions. The records must be properly stored, preserved and available for access.

1.3 The purpose of this policy is to facilitate the proper creation, management, preservation and disposal of e-mail records.

1.4 All employees of Richtersveld Municipality shall implement the e-mail policy.

2. Policy statement

2.1 All records created and received by Richtersveld Municipality shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 1996.

2.2 The following broad principles apply to the record keeping and records management practices of Richtersveld Municipality:

- The Richtersveld Municipality follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
- The records management procedures of Richtersveld Municipality comply with legal requirements, including those for the provision of evidence.
- The Richtersveld Municipality follows sound procedures for the security, privacy and confidentiality of its records.
- Electronic records in the Richtersveld Municipality are managed according to the principles promoted by the National Archives and Records Service.
- The Richtersveld Municipality has performance measures for all records management functions and reviews compliance with these measures.

3. Relationship with other policies

3.1 The Richtersveld Municipality's, e-mail management policy are related to the

- Official e-mail system use policy;
- Records management policy;
- Electronic records management policy; and
- Web content management policy
- Document imaging policy.

3.2 Other policies that are closely related to the e-mail management policy are

- the information security policy that is managed by the security manager;
- the internet usage policy that is managed by the IT manager; and the
- the promotion of access to information act that is managed by the Chief Information Officer.

4. Scope and intended audience

4.1 Applicability to employees

4.1.1 This policy applies to all staff of Richtersveld Municipality who generate records while executing their official duties.

4.1.2 Employees of Richtersveld Municipality should be aware that e-mails are subject to Promotion of Access to Information (PAIA) requests and legal discovery when a lawsuit is pending. Should e-mails that are a subject of a PAIA request or legal discovery be deleted because e-mails are not managed properly Richtersveld Municipality will face severe court sanctions and/or a criminal charge.

4.1.3 Employees who willfully contravenes the e-mail management provisions in this policy will face disciplinary action.

4.2. Applicability to e-mails as records

4.2.1 E-mails that are evidence of the business transactions of Richtersveld Municipality are public records and shall be managed and kept for as long as they are required for functional and/or historical purposes.

4.2.2 E-mails that 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, contain policy decisions, etc. should be managed as records and should be filed into the file plan. This policy covers the e-mail message itself as well as any attachments that meet these criteria.

4.2.3 An e-mail message is a record if it:

- contains unique, valuable information developed in preparing position papers, reports, studies, etc.
- reflects significant actions taken in the course of conducting business.
- conveys unique, valuable information about Richtersveld Municipality's programs, policies, decisions, or essential actions.
- conveys statements of policy or the rationale for decisions or actions.
- documents oral exchanges (in person or by telephone), during which policy is formulated or other business activities are planned or transacted.
- adds to the proper understanding of the formulation or execution of Richtersveld Municipality's actions or of Richtersveld Municipality's operations and responsibilities.
- documents important meetings.

- facilitates action by Richtersveld Municipality's officials and their successors in office.
- makes possible a proper scrutiny by the Auditor-General or other duly authorized agents of the government.
- protects the financial, legal, and other rights of the Richtersveld Municipality and of the persons directly affected by the Richtersveld Municipality's actions.
- approves or authorizes actions or expenditure.
- constitutes a formal communication between staff e.g. correspondence or memoranda relating to official business.
- signifies a policy change or development.
- creates a precedent e.g. by issuing an instruction or advice.
- involves negotiations on behalf of the Richtersveld Municipality.
- has value for other people or the Richtersveld Municipality as a whole.

4.2.4 E-mails that contain the following do not need to be filed:

- meeting announcements.
- announcements of employees' absences or schedules.
- changes in telephone numbers or office locations.
- meeting arrangements that normally would have been done by telephone.
- copies of memoranda or text sent for information rather than action.
- messages that have only temporary value such as a message that a meeting time has changed.
- messages that contain no evidence of Richtersveld Municipality's functions and activities.
- duplicate information already documented in existing records.

5. Regulatory framework

5.1 By managing its e-mailed records effectively and efficiently Richtersveld Municipality strives to give effect to the actability, transparency and service delivery values contained in the legal framework established by:

- Constitution, 1996;
- National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended);
  - National Archives and Records Service of South Africa Regulations;
- Public Finance Management Act (Act No 1 of 1999);
- Promotion of Access to Information Act (Act No 2 of 2000);
- Promotion of Administrative Justice Act (Act No 3 of 2000);
- Electronic Communications and Transactions Act (Act No 25 of 2002).

6. Roles and responsibilities

6.1 Top management

6.1.1 Top management is responsible for the approval of this policy and for the designation of a senior manager as the records manager. Top management shall mandate the records manager to implement this policy.

6.1.2 Top management shall ensure that the management of records including e-mail is a key responsibility in the performance contracts of all senior managers.

6.2 Senior manager

6.2.1 Senior managers are responsible for the implementation of this policy in their respective units. They shall ensure that the management of records including e-mail is a key responsibility in the performance agreements of all the staff in their units.

6.2.2 Senior managers shall lead by example and shall ensure that records, including e-mail generated by them are managed properly.

6.3 Records manager/Head of Corporative Services

6.3.1 The records manager is responsible for:
- the implementation of this policy;
- staff awareness regarding this policy.

6.3.2 The records manager is responsible for ensuring that e-mails are managed as records according to the records management principles prescribed by the National Archives and Records Service Act and in terms of this policy. In this regard the records manager shall be consulted to determine which types of e-mail would be considered official records that should be managed properly, if the specific types are not covered in par. 3 above.

6.3.3 The records manager shall ensure that all records created and received by Richtersveld Municipality are classified according to the approved file plan and that a written disposal authority is obtained for them from the National Archives and Records Service.

6.3.4 The records manager is responsible for determining retention periods in consultation with the risk manager, the legal services manager and the users and taking into account the functional, legal and historical need of the body to maintain records of transactions.

6.3.5 The records manager is mandated to make such training and other interventions as are necessary to ensure that the Richtersveld Municipality's record keeping and records management practices comply with the records management principles contained in the National Archives and Records Service Act.

6.3.6 The records manager may from time to time issue circulars and instructions regarding the record keeping and records management practices of Richtersveld Municipality.

6.3.7 The Head of Corporative Services is the records manager for the whole Richtersveld Municipality.

6.3.8 The records manager shall monitor the implementation of this policy.

6.4 Chief Information Officer

6.4.1 The Chief Information Officer is responsible for approval of requests for information in terms of the Promotion of Access to Information Act.

6.4.2 The Chief Information Officer shall inform the records manager if a request for information necessitates a disposal hold to be placed on records that are due for disposal.

6.5 IT manager

6.5.1 The IT Manager is a sub records manager and he/she is responsible for the day-to-day maintenance of electronic systems that stores records including the (hardware/software) that serves as the conduit for receiving and transmitting e-mail.

6.5.2 The IT manager shall work in conjunction with the records manager to ensure that public records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes.

6.5.3 The IT manager shall ensure that no e-mails are deleted from any system without consulting the records manager.

6.5.4 The IT manager shall ensure that the integrity of any records housed in the e-mail is protected until they have reached their approved retention. Integrity of these record will be accomplished through such procedures as test restores, media testing and data migration and capturing the required audit trails.

6.5.5 The IT manager shall ensure that appropriate systems technical manuals and systems procedures manuals are designed for each electronic system that manages and stores records.

6.5.6 The IT manager shall ensure that all electronic systems capture appropriate systems generated metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created.

6.5.7 The IT manager shall ensure that electronic records in all electronic systems remains accessible by migrating them to new hardware and software

platforms when there is a danger of technology obsolescence including media and format obsolescence.

6.5.8 The IT manager shall ensure that all data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.

6.5.9 The IT manager shall ensure that the back-up files for the e-mail system are recognized as being part of the overall records management system in that the subject classification scheme shall be evident if files need to be retrieved from the backups.

6.5.10 The IT manager shall ensure that back-ups are stored in a secure off-site environment.

6.5.11 The IT manager shall ensure that systems that manage and store records are virus free.

6.5.12 Further comprehensive details regarding specific responsibilities of the IT manager are contained in:

- the electronic records management policy;
- the e-mail policy;
- the web content management policy;
- document imaging policy; and the
- information security policy.

6.6 Security manager

6.6.1 The security manager is responsible for the physical security of all records.

6.6.2 Details regarding the specific responsibilities of the security manager are contained in the Information Security Policy.

6.7 Legal services manager

6.7.1 The legal services manager is responsible for keeping the records manager updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of Richtersveld Municipality.

6.8 Staff

6.8.1 Every user of the official e-mail system is responsible for ensuring that e-mails, that are evidence of business transactions, are captured as records.

6.8.2 Every user of the official e-mail system is responsible for ensuring that e-mails a subject classified against the approved file plan.

7. Filing e-mails

7.1 E-mails shall under no circumstances be isolated from Richtersveld Municipality's records management systems. They shall be captured into the file plan contained in the Integrated Document and Records Management System.[1] E-mails and attachments shall be captured as separate but linked records.

7.2 If an e-mail impacts on the work of a user and it complies with the criteria stated in par. 3, the e-mail shall be filed by the sender except if:

- there is a person in a unit or project group to whom the responsibility for this task has been designated.
- it is an e-mail received from outside the (name of governmental body) in which case the recipient is responsible for filing it.

8. Disposing of e-mails

8.1 E-mails considered to be public records shall not be deleted or otherwise disposed of without a written disposal authority issued by the National Archivist.

8.2 E-mails filed to subject files in the file plan are covered by Standing Disposal Authority No (insert number issued by the National Archives and Records Service) and shall be disposed of according to the retention periods in that disposal authority.

8.3 Should an e-mail be received/generated for which an appropriate subject file does not exist in the file plan, the records manager should be contacted to add an appropriate subject to the file plan and to apply for disposal authority on that subject.

8.4 E-mails that are not public records may be disposed of after (governmental body should decide how long) months in terms of the National Archives and Records Service's General Disposal Authority AT2 for the Destruction of Transitory Records.

9. Creating reliable e-mail records

9.1 Structuring an out-going e-mail

9.1.1 E-mails that are public records shall contain sufficient information to ensure that they are properly contextualized and that they are meaningful and accessible over time.

9.1.2 Outgoing mail shall include the reference number of the subject folder in the

file plan in the top right hand corner of the message box to provide a contextual link to the business activity that supports the e-mail.

9.2 Proper subject line

9.2.1 Subject lines are very important, since they indicate to a recipient what the message is all about. If subject lines are not used appropriately, the recipients may not realize the importance of the message and choose to read it later or not at all. Users shall allocate useful subject lines to e-mails.

9.2.2 If a user receives a message with a senseless subject line and needs to reply to or forward it, the subject line should be changed to properly cover the subject of the e-mail before sending it off.

9.3 Auto-signatures

9.3.1 Staff should always be contactable even if their e-mail systems are down. Auto-signatures shall be used and shall contain the following identifying information of a sender:

- name of sender
- position of sender
- name of unit/section
- name of the governmental body
- postal address
- phone number
- fax number

9.4 Attachments

9.4.1 If an outgoing mail includes an attachment, the attachment shall be filed into the file plan in the Integrated Document and Records Management System before it is attached to the e-mail to ensure that it contains the following prescribed minimum mandatory metadata.

- File plan reference number
- Record title: A sensible name given to it by the user
- Author
- Originating organization
- Originating sub office
- Record date
- Record type

9.4.2 Attachments shall be virus free.

10. Language used in e-mails

10.1 Official communications shall be approached in the same manner as a business letter, thinking it through carefully and using proper grammar and

correct spelling.

11. Capturing e-mail string

11.1 E-mail messages on a particular subject can become a string of replies until a matter is finalized. In such cases users shall:

- place all e-mails into the system separately as they occur and relate them to each other or
- capture the final message – in which case user needs to make sure that the final message contains whole thread of the discussion.

12. When to capture e-mails

12.1 Users shall capture official e-mails at the time of the action to ensure that

- the chronological order of the business transaction is clear.
- the authenticity of e-mail is guaranteed.

13. Metadata

13.1 The IT manager shall ensure that the system is set up to capture the following metadata:

- The transmission data that identifies the sender and the recipient(s) and the date and time the message was sent and/or received;
- When e-mail is sent to a distribution list, information identifying all parties on the list must be retained for as long as the message is retained.

14. Monitor and review

14.1 The records manager shall review the e-mail record keeping and records management practices of [name of governmental body] on a regular basis and shall adapt them appropriately to ensure that they meet the business and service delivery requirements of Richtersveld Municipality.

14.2 This policy shall be reviewed on a regular basis and shall be adapted appropriately to ensure that it meets the business and service delivery requirements of Richtersveld Municipality.

15. Definitions

Correspondence system:

A set of paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.

Disposal:

The action of either destroying/deleting a record or transferring it into archival custody.

Disposal authority:

A written authority issued by the National Archivist specifying which records should be transferred into archival custody or specifying which records should be destroyed/deleted or otherwise disposed of.

Disposal authority number:

A unique number identifying each disposal authority issued to a specific office.

Electronic records:

Information which is generated electronically and stored by means of computer technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

Electronic records system:

This 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 meta data (background and technical information i.r.o. the information stored electronically) and in hard copy. All these components are defined as records by the Act. They must therefore be dealt with in accordance with the Act's provisions.

File plan:

A pre-determined classification plan by which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.

Public record:

A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

Record:

1) Recorded information regardless of form or medium.

2) Evidence of a transaction, preserved for the evidential information it contains.

Record keeping:

Making and maintaining complete, accurate and reliable evidence of official business in the form of recorded information.

Records management

Records management is a process of ensuring the proper creation, maintenance, use and disposal of records throughout their life cycle to achieve efficient, transparent and accountable governance.

Retention period:

The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.

System technical manual:

A manual containing information regarding the hardware, software and network elements that comprise the system and how they interact. Details of all changes to a system should also be documented.

System procedures manual:

A manual containing all procedures relating to the operation and use of the electronic system, including input to, operation of and output from the system. A system procedures manual would contain detailed procedures regarding -

- Document capture
- Document scanning
- Data capture
- Indexing
- Authenticated output procedures
- File transmission
- Information retention
- Information destruction
- Backup and system recovery
- System maintenance
- Security and protection
- Use of contracted services
- Workflow
- Date and time stamps
- Version control
- Maintenance of documentation

A systems procedures manual should be updated when new releases force new procedures.

16. References

National Archives and Records Service: *Records Management Policy Manual*, April 2006.

National Archives and Records Service: Managing electronic records in governmental bodies: Policy, principles and requirements, April 2006.

National Archives and Records Service: Performance criteria for records managers in

governmental bodies, April 2006.

National Intelligence Agency: Minimum Information Security Standard.

South African Bureau for Standards: SANS 15489: Information and documentation – Records management – Part 1: General.

South African Bureau for Standards: SANS 15489 Information and documentation – Records management – Part 2: Guidelines.

South African Bureau for Standards: SANS 15801: Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability.

South African Bureau for Standards: SANS 23081: Information and documentation – Records Management processes – Metadata for records – Part 1: Principles.

South African Bureau for Standards: SANS 17799: Information Technology – Security techniques - Code of Practice for Information Security Management.

17. Authorization

APPROVED DATE	**2 JULY 2019**
EFFECTIVE DATE	**1 JULY 2019**
REVIEW DATE	**30 JUNE 2020**
COUNCIL RESOLUTION	**RVM 06/07/2019**
SIGNATURE OF MUNICIPAL MANAGER