Records and information Management Policy

POL_MER_003

Version 1.0 2022/23

Version Control and Approval	
Document Name	**Records and information management Policy**
Year of Current Review	2022/2023
Year of Next Review	2023/2024
Compiled by Information Management Centre (IMC) Practitioner	
Name of the IMC Practitioner	Mr. Rishaan Govender
RGovender Signature:	Date: 10 November 2022
Reviewed by Manager: Monitoring, Evaluation and Reporting (MER)	
Name of the MER Manager	Ms. Melanie Rajagopal
Rajagopal Signature:	Date: 10 November 2022
Recommended by Executive Manager: Skills Planning & Research	
Name of the Executive Manager	Mr. Vukani Memela
Signature:	Date: 23/11/2022
Approved by CEO	
Name of the CEO	Mr. Thamsanqa Mdontswa
Signature:	Date: 24/11/2022

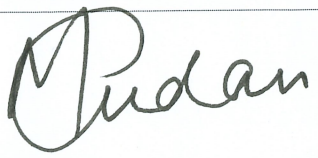
Approved by Chairperson of the Accounting Authority	
Name of the Chairperson	Mr Chris Mudau
Signature: 	Date: 24/11/2022

Table of Contents

Executive Summary

SASSETA's Records and information management Policy draws its mandate from the National Archives and Records Services of South Africa Act (Act No. 43 of 1996) and various legislative and regulatory instruments. It is also informed by SANS I 5489: Records Management and the Minimum Information Security Standards (MISS), and other guidelines as recommended by the National Archivist.

In terms of the National Archives and Records Services of South Africa Act, (Act No. 43 of 1996) statutory bodies such as **SASSETA** are required to establish and maintain a records management programme that conforms to standards and codes of best practice in records management approved by the National Archivist.

The policy defines the way **SASSETA's** documents and records should be managed according to prescribed legislations and standards. It further provides a framework for proper records management practices to cover all **SASSETA** records, both present and future, in whichever media format that they have been captured in, e.g., paper, electronic, audio-visual, etc.

This policy should be read in conjunction with the following critical legislation, policies, and standards applicable to SASSETA:

Legislation	Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996);
	National Archive and Records Services of South Africa Act, 1996 (Act No. 43 of 1996);
	Public Finance Management Act, (Act No. 1 of 1999);
	Public Audit Act, 2004 (Act No. 25 of 2004);
	Promotion of Access to information Act, 2000 (Act No. 2 of 2000);
	Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000);
	Electronic Communication and Transaction Act, (Act No. 25 of 2002);
	Protection of Personal Information Act; 2013 (No. 4 of 2013);
Policies	IT Governance Framework, Electronic Communication Policy, IT Security policy, Code of Ethics.

Procedures	Records Management SOP
Standards	Minimum Information Security Standards, 1996; SANS: 15489:2001 Information and Documentation – Records Management

Definitions

Archives	Records in the custody of an archives repository
Archival Value	Those value, administrative, fiscal, legal, evidential and/ or informational, which justify the indefinite or permanent retention of records.
Disposal authority	A written authority issued by the national archivist specifying records to be transferred into archival custody or specifying records to be destroyed/deleted.
Document	Recorded information or objective which can be treated as a unit.
Electronic Document Management System	A system that provides the ability to capture, describe and categorise, store, retrieve, share and reuse electronic documents regardless of specific format.
Electronic records	Information that is generated electronically and stored by the means of computer technology.
File plan	A predetermined classification plan by which records are filed and/ or electronically indexed to facilitate efficient retrieval and disposal of records.
MISS	Minimum Information Security Standard (MISS) is an official government policy document (approved by Cabinet) dealing with information security.
Records	Recorded information regardless of form or medium. As defined in the National Archives and Records Services of South Africa Act, No. 43 of 1996 as amended.
Record Classification System	A plan for the systematic identification and arrangement of business activities and/ or records into categories according to logically structured conventions, methods and procedural rules represented in the classification system.
Record keeping	Creating and maintaining complete, accurate and reliable evidence of official business in the form of recorded information.

Record Keeping System	A collection of policies procedures and systems, which capture information according to a records classification system, manage, store and provide access to records and their context over time.
Records Manager	A SASSETA Document and Records Management Specialist appointed in terms of section 13 (5) (a) of the National Archives and Records Services of South Africa Act, 1996 (Act No. 43 of 1996).
Retention period	The length of time (as regulated by legislation) that records should be retained by SASSETA before they are either transferred to archival custody or destroyed/deleted

1. Introduction

Information management is critical to **SASSETA's** core business of skills development within the safety and security sector. The records that **SASSETA** generates during the implementation of its business strategy represents and provides evidence of achievement in relation to its targets. Organisations that manage information effectively are better at handling their assets, understanding their customers and benchmarking of critical processes. It is therefore imperative that **SASSETA** develops its information management capability and competency.

SASSETA should view the information that resides in documents and records as a strategic asset that can assist the organisation to increase its business effectiveness and efficiency while ensuring that all evidentiary and legislative compliance factors are met. Non-compliance, unauthorised access to **SASSETA's** information including theft, loss or damage thereof may lead to reputational risk.

2. Purpose

The purpose of this policy is to:

2.1 Regulate documents and records management practices within **SASSETA** and align them to the requirements of the National Archives and Records Service Act, 1996 (No. 43 of 1996) (as amended), Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (PAIA) and other related legislation.

2.2 Provide guidelines to **SASSETA** employees on the creation, receipt, access, organising, use, storage, retrieval and disposal of records.

2.3 Ensure protection of **SASSETA's** reputation through compliance with the legal retention periods of records as prescribed by legislation.

2.4 Ensure confidentiality, safe custody, integrity, accessibility and easy retrieval of all **SASSETA** documents and records in accordance with Protection of Personal Information Act.

2.5 Provide a framework for proper document and records management practices to cover all **SASSETA's** documents and records, both present and future, in whatever media format they have been captured, e.g., paper, electronic, audio visual, etc.

3. Policy statement

All documents and records created and received by **SASSETA** shall be managed in accordance with this policy and the records management principles contained in section 13 of the National Archives and Records Services Act, 1996 (Act No. 43 of 1996) and other related legislations.

4. Roles and responsibilities

4.1 Chief Executive Officer (CEO)

4.1.1 The CEO is ultimately accountable for the documents and records management practices of **SASSETA.**

4.1.2 The CEO is the Information Officer in terms of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (PAIA).

4.1.3 The Information Officer is responsible for approval of request for access to information or his/her delegated authority.

4.1.4 The information officer is further responsible for:

- The secure retention of records, as such in the event of a security breach the information owner will be notified as per the SASSETA breach response procedure.

- Records retained by SASSETA may be processed multiple times to enable the SASSETA business processes.

- All records are classified as special records and are protected with the industry leading information security controls as per the best practice recommendation.

4.1.5 The Information Officer shall designate in writing a Deputy Information Officer (DIO) to handle PAIA requests.

4.1.6 The procedure for request for access to Information is contained in **SASSETA** PAIA manual, which will be made available on the **SASSETA** website upon approval.

4.2 Deputy Information Officer (DIO)

4.2.1 All Executive Managers have been appointed as Deputy Information Officers (DIO) and are responsible for information management in their respective portfolios.

4.2.2 The DIO is responsible for the approval of requests for information in terms of the Promotion of Access to Information Act.

4.2.3 The DIO must inform the Records Manager if a request for information necessitates a disposal hold to be placed on records that are due for disposal.

4.2.4 DIOs must enforce compliance with this policy.

4.3 Monitoring, Evaluation and Reporting (MER) Manager

The MER manager is accountable for the development of a SASSETA Document and Records Management policy with procedures.

4.3.1 He/she is accountable for advocating policies and procedures on Information and knowledge management.

4.3.2 He/she is accountable for establishing the records management committee for governing, monitoring and implementation of documents and records management activities within **SASSETA.**

4.3.3 Accountable for the implementation and monitoring of this policy.

4.3.4 Accountable for staff awareness and training regarding this policy.

4.3.5 Accountable for the determination of retention periods for all **SASSETA** records in accordance with relevant legislation.

4.3.6 The Records Manager is accountable for coordinating and reporting on PAIA section 32 to the South African Human Rights Commissioner at the end of the financial year.

4.3.7 The Records Manager should successfully complete the National Archives and Records Service's Records Management Course, as well as any other records management training to equip him/her for his/her duties.

4.4 Department Managers

4.4.1 Managers of Departments are responsible for the implementation of this policy within their respective business areas.

4.4.2 Managers of Departments must ensure that all staff members within their business areas are aware of this policy.

4.4.3 Managers of Departments must enforce compliance with this policy.

4.4.4 Managers of Departments must lead by example by maintaining proper records management and document practices.

4.4.5 Managers of Departments shall designate records champions for their respective Departments, responsible for assisting with the implementation of this policy within their business areas. Furthermore, managers are responsible for providing retained records to the respective records owner upon receipt of a formal request of records by the owner.

4.4.6 Managers are responsible for ensuring that records retained by SASSETA remain unaltered, accurate, valid and complete as per original received record.

4.4.7 Managers of Departments are responsible for providing information pertaining to PAIA requests to the **Deputy Information Officer** within the requested time period. This must be done in consultation with the Records Manager and GRC unit.

4.4.8 GRC Manager is responsible for keeping the IMC Practitioner updated on developments in the legal and statutory environment that may impact on the records management practices of **SASSETA.**

4.4.9 The GRC office must keep an inventory of all SASSETA policies and procedures.

4.5 Information Management Centre (IMC) Practitioner

4.5.1 The IMC Practitioner is responsible for the development of a SASSETA Records Management Policy with procedures.

4.5.2 Responsible for the implementation and monitoring of this policy.

4.5.3 Responsible for staff awareness and training regarding this policy.

4.5.4 Responsible for the determination of retention periods (in consultation with the Records Manager) for all **SASSETA** records in accordance with relevant legislation.

4.6 Information Technology (IT) Manager

4.6.1 The Information and Technology (IT) Manager is responsible for the day-to-day maintenance of approved electronic systems that store documents and records.

4.6.2 The IT Manager shall ensure that documents and records in all electronic systems remain accessible by migrating them to new hardware and software platforms when there is a remain danger of technology obsolescence, including media and format obsolescence.

4.6.3 The IT Manager shall ensure that all data, metadata, audit trial data, operating systems and application software is backed up on a regular basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.

4.8 IMC Staff

4.8.1 The IMC staff are responsible for the management of physical records in their care.

4.8.2 Detailed responsibilities regarding the day-to-day management of the records in the IMC are contained within the Records Management SOP.

4.8.3 Record retrievals will follow the below timeframe:

Record Type	Time frame	Emergency
Onsite Storage	48 hrs	24 hrs
Offsite Storage	72 hrs	36 hrs
Digital Space	24 hrs	12 hrs

4.9 All SASSETA staff members

4.9.1 All staff members must create documents and records of transactions while conducting official **SASSETA** business and manage them according to the SASSETA file plan, once approved.

4.9.2 All staff members shall manage the documents and records efficiently and effectively by:

a) Sending paper-based records to their allocated storage rooms for safekeeping.
b) Ensuring that electronic documents and records are managed according to the requirements of the IT policies and information classification procedures.
c) Adhering to the "Clean Desk" principle; and
d) Ensuring that records are destroyed/deleted in accordance with the disposal authority issued by the National Archivist.

5. Custody of Documents and Records

All items pertaining to the custody of documents and records including storage facilities of offsite records as well as electronic will be detailed in the Records Management SOP.

6. Information ownership

6.1 All records, irrespective of the format, created by any person or entity in the service of **SASSETA,** are owned by **SASSETA** and subject to its overall control. This includes **SASSETA** staff, clients and independent contractors.

6.2 Where custody of **SASSETA** records passes to a contracted service provider through outsourcing or any other arrangement, the records will remain the property of **SASSETA** and will be subject to approved disposal instructions and storage requirements.

6.3 Employees leaving **SASSETA** or changing positions within **SASSETA** must leave all documents and records for their successors.

7. Records classification system

All items pertaining to the records classification system and Electronic Document and Records Management (EDRMS) will be detailed in the Records Management SOP.

8. Protection of Personal Information (POPI)

The details of POPI can found in the POPI policy which resides in the custody of the GRC department. Quote ref POPI_GRC_001

9. Disposal of records

9.1 No **SASSETA** records will be destroyed, erased or otherwise disposed of without prior written authorisation from the National Archivist.

9.2 The MER department shall request a standing disposal authority from the National Archivist.

9.3 Once a disposal authority is obtained, the IMCP, line functionaries and legal advisers shall determine retention periods on the file plan, taking **SASSETA's** legal obligations and functional needs into account. The records retention schedule must be published on the intranet and maintained by the MER department.

9.4 Disposal in terms of these disposal authorities shall be executed once annually in April.

9.5 All records that are no longer necessary to enable SASSETA business processes may be destroyed more frequently to ensure that records are kept on a need to have basis, unless specified otherwise by the National Archives Act/ SANS requirements.

9.6 All disposal actions shall be verified by the MER manager prior to their execution to ensure that archival records are not destroyed accidentally.

10. Access and security classification

All items pertaining to the access and security classification of records will be detailed in the Records Management SOP.

11. Clean Desk Policy

11.1 All staff must allocate time to ensure that their desks are clean and that all paperwork is filed in accordance with the Records Management SOP.

11.2 All staff members must clear their workspace before leaving for longer periods of time.

11.3 All staff members must make use of the shredders for sensitive documents when they are no longer needed.

11.4 All staff members must lock their desks and filing cabinets at the end of the day.

11.5 Laptops must be securely locked at all times.

11.6 Sensitive and confidential documents and other devices that store information, such as USBs, CDROMs, DVDs, and Hard Drives must be locked away when not in use.

11.7 Managers of Departments must ensure that the clean desk policy is adhered to.

12. Inspections

12.1 The MER manager shall conduct records inspections at all **SASSETA** offices on quarterly basis and audits on annual basis to assess compliance with this policy and report to the records management committee.

12.2 The internal audit function shall on a regular basis, carryout an audit to assess compliance with the policy and other related legislations.

13. Non-compliance

13.1 No deviation from this policy shall be allowed without written authorization by the CEO.

13.2 Non-compliance with the Records Management policy provision will lead to actions as contained in the **SASSETA** disciplinary policy.

14. Application of this policy

This policy is applicable to all:

a) **SASSETA** departments, regional offices, and staff,
b) Documents and records created by **SASSETA** owned subsidiaries,
c) Documents and records created by suppliers contracted by **SASSETA**; and
d) Documents and records created or received by **SASSETA** regardless of format or medium.

15. Policy updates

15.1 This policy shall, if necessary, be reviewed annually and updated in response to internal or external stimuli such as changes in operating practice, regulatory environment or standards.

15.2 The revision of the policy shall be communicated through the appropriate formal organisational communication channels.

16. Delegations of authority

16.1 All the documentation forwarded to management must not be approved without a file plan reference number.

16.2 The disposal of records shall be acknowledged by the managers of the respective departments and executed by the MER department.

16.3 Access to confidential files can only be granted with approval from the manager of the respective department who is the owner of the record.

16.4 Requests of access to records in terms of PAIA by members of the public must be approved by the designated Deputy Information Officer.