

Information and Records Management Policy

Document Number:	8/6/P
Approved By:	Board of Directors
Approval Date:	March 2019
Next Review Cycle:	December 2022
Version:	1.0
Type:	Governance
Policy Owner:	Executive Manager: Governance and Secretariat
Oversight:	Social and Ethics Committee AND Board

**This document has been issued strictly for internal business purposes of Sasria.
All rights including those in copyright in the content of this document are owned by Sasria.**

Table of Contents

1. Introduction.....	3
2. Policy Statement.....	3
3. Relationship with other policies	3
4. Regulatory Framework	4
5. Definitions	5
6. Purpose of Policy.....	6
7. Policy Principles	6
8. Classification of documents and records	8
9. Storage and caring for records.....	8
10. Access and security	8
11. Managing email records	9
12. Email of departing staff members.....	9
13. Clean desk practices	9
14. Disposal of records	10
15. Version Control (Detailed guidance on version control will be included in the procedures).....	10
16. Retention Schedule	10
17. Key monitoring controls.....	11
18. Roles and Responsibilities.....	11
19. Applicability to employees	11
20. Delegations of Authority	11
21. Failure to Apply or Comply with the Policy.....	11
22. Revision of the policy	12

1. Introduction

Sasria views its information and records as a valuable asset. Appropriate records management is vital to the maintaining and enhancing the value of this asset. Sasria has developed this policy to highlight and ensure compliance with information and data security requirements. In addition, records management, through the proper control of the content, storage and volume of records, reduces the vulnerability to legal challenge and financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

Sasria is also required to align its procedures and processes with records, data and information protection laws. The policy applies to all who receive, create, have access to, manage, store and dispose records, including electronic records.

As an internal control, the policy provides directors and executives with the assurance that records management, retention, disposal and business continuity risks are being managed and mitigated within Sasria.

This policy must be read in conjunction with Human Capital Policies, Operational Risk Management Policy, and Information Technology and Security policies.

2. Policy Statement

It is the policy of Sasria to manage its records in an accountable, effective and efficient manner through the implementation of a records management programme that takes into account related objectives such as orderly classification of records, retention and disposal, accessibility, security and confidentiality, training performance and quality management.

Sasria is committed to protecting records and documents that contain sensitive information of the company, customers, employees, suppliers and contractors.

To this end –

- (a) All records received or created by Sasria shall be managed, protected and disposed of in line with the regulatory framework applicable to this policy.
- (b) Sasria shall follow sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
- (c) The records management procedures of Sasria comply with legal requirements.
- (d) Sasria shall follow sound procedures for the security, privacy and confidentiality of its records.
- (e) Sasria shall have performance measures for all records management functions and will review compliance with these measures.

3. Relationship with other policies

- a) Sasria's Information and Records Management Policy consist of this policy as well as additional parts that cover the unique nature of the broad spectrum of records generated by Sasria Organisation. These policies are managed by the records manager.
- b) Other policies that are closely related to this Policy are:

- the Information Technology and Security Policy which is managed by the Information Security Officer.
- The Usage Policy which is managed by the IT Manager.

4. Regulatory Framework

The regulatory framework for the Records Management and Retention Policy is provided by:

- i. King IV Report on Corporate Governance for South Africa, 2016
- ii. Protection of Personal Information Act, No. 4 of 2013
- iii. Tax Administration Act, No. 28 of 2011
- iv. Consumer Protection Act, No. 68 of 2008
- v. Securities Transfer Tax Administration Act, No. 26 of 2007
- vi. Auditing Profession Act, No. 26 of 2005
- vii. Financial Advisory and Intermediary Services Act, No. 37 of 2002
- viii. Electronic Communications and Transactions Act, No. 25 of 2002
- ix. Unemployment Insurance Act, No. 63 of 2002
- x. Financial Intelligence Centre Act, No. 38 of 2001
- xi. ISO 15489-1:2001, clause 6.2.
- xii. Promotion of Administrative Justice Act, No. 3 of 2000
- xiii. Promotion of Access to Information Act, No. 2 of 2000
- xiv. Public Finance Management Act, No. 1 of 1999
- xv. Employment Equity Act, No. 55 of 1998
- xvi. Basic Conditions of Employment Act, No. 75 of 1997
- xvii. Legal Deposits Act, No. 54 of 1997
- xviii. Constitution of the Republic of South Africa, 1996
- xix. National Archives and Records Services of South Africa Act, No. 43 of 1996
- xx. Labour Relations Act, No. 66 of 1995
- xxi. Compensation for Occupational Health and Diseases Act, No. 130 of 1993
- xxii. Occupational Health and Safety Act, No. 85 of 1993
- xxiii. Value Added Tax, No. 89 of 1991
- xxiv. Income Tax Act, No. 58 of 1962
- xxv. Transfer Duty Act, No. 40 of 1949

5. Definitions

Archiving:	Archiving is the process of permanently preserving selected records that are no longer required for current business use.
Authentic records:	Authentic records are records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.
Authoritative records:	Authoritative records are records that are authentic, reliable, trustworthy and useable and are complete and unaltered
Correspondence system:	A set of paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.
Data management:	Administrative process by which the required data is acquired, validated, stored, protected, and processed, and by which its accessibility, reliability, and timeliness is ensured to satisfy the needs of the data users.
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, programs and metadata 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.
Information security:	Information security, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of <u>information</u> .
	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, which 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.
Version control	Version control, also known as revision control or source control, is the management of changes to documents, and other collections of information. Changes are usually identified by a number or letter code, termed the "revision number", "revision level", or simply "revision".
Vital record	Document, record or file in any format with information essential, necessary to create and organise operations and survival of an organization

6. Purpose of Policy

Records management policy outlines the principles, practices and procedures for the Management of Sasria's records.

The purpose of this policy is to:

- a) Regulate documents and records management practices within Sasria and align them with relevant legislation.
- b) Provide direction to Sasria employees on the registration, creation, approval, receipt, access, organisation, storage, use and disposal of documents, information and records
- c) Ensure that Sasria is protected by complying with the records and information management legislation.
- d) Ensure confidentiality, privacy, security, integrity, accessibility and retrievability of all Sasria employees' information and records among others, to ensure the safety of all important and sensitive documents and information. The policy further ensures ease of access to records and information, as required by Sasria. This will ensure efficient and effective execution of its functions. The policy further ensures continuity in the event of a disaster and protects the rights and interests of employees, clients, and other present and future stakeholders.

7. Policy Principles

This policy is developed based on the following principles that govern and support Sasria's record management, record keeping and data retention practices:

- (a) Documents and records must be managed properly from creation to disposal.

- (b) Sasria follows sound procedures and practices for the creation, receiving, maintenance, retention and disposal of all records and data, including electronic records.
- (c) The records management procedures will comply with legal requirements, including those for provision of evidence in court, where applicable.
- (d) Sasria will follow sound procedures for the security, privacy and confidentiality of its data, records, as well as personal information at its disposal.
- (e) Electronic records of Sasria will be managed in line with the requirements of the National Archives and Records Service of South Africa.
- (f) Sasria will have performance measures in place for all records management functions and conduct regular compliance reviews with these performance measures.
- (g) Adoption of the records management and retention policy by the board or delegate of the board.
- (h) Development of records management and retention procedures and processes by the relevant Executive Manager, and implementation thereof by Sasria management and staff.
- (i) Availability of lockable storage and shredding facilities for use by all employees.
- (j) Identification, assessment and management of records, data and information security risks.
- (k) Monitoring of compliance with policy and reporting of areas of concern and / or non – compliance.
- (l) Reporting of incidents and information security near-misses per Sasria’s Operational Risk Management Policy - Loss Data Collection.
- (m) Training of staff to ensure awareness on the policy and its attendant procedures and processes.
- (n) Implementing safe disposal methods for data and documents containing company, customer and supplier sensitive and personal information.
- (o) Valuable documents and records must be secured at all times.
Documents and records must be accessible to authorised employees for business purposes.
- (p) Sasria’s records and documents must be securely stored and preserved in a proper manner.
- (q) Implementation of internal controls by management to ensure that such controls are operating effectively to deter and detect areas of non – compliance with the policy.
- (r) staff being alert and actively participating in proper document and information management and security.
- (s) Some records may be disposed of or destroyed within five years and some may have to be kept per the retention schedule.
- (t) The purpose of this policy is to provide guidelines to all company employees on how to treat specific types of information, what confidentiality levels apply to what information classes, and especially what information may be shared with external parties.
- (u) Sasria personnel are encouraged to use good judgment in securing Sasria Confidential information to the proper extent - if an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

8. Classification of documents and records

- a) All confidential documents and records created within Sasria must be classified or reclassified or declassified by an executive manager.
- b) All secret and top secret documents and records, created within Sasria must be classified or reclassified or declassified by the Managing Director as per the classification schedule
- c) When there is a need to re-classify or de-classify documents or records received, an employee of Sasria must consult the relevant Executive Manager prior to obtaining written authorisation from the Managing Director.
- d) Original top secret and secret records must be kept for the purpose for which it was collected and thereafter should be transferred to Company Secretary for safe keeping.
- e) Only declassified records may be made available to the public through the PAIA.

9. Storage and caring for records

- a) All Sasria records shall be kept in storage areas or facilities that are appropriate for the type of medium as per the file plan.
- b) A record must only be kept in paper-based format in cases where it is deemed extremely necessary to keep it in its original form.
- c) This record must be kept in the creator's allocated storage for a period of one year and then transferred to a Sasria storage facility.

10. Access and security

- (a) Records shall at all times be protected from unauthorised access, movement and tempering with, to sustain their authenticity and reliability.
- (b) No Sasria employee may remove documents and records that are not available in the public domain from Sasria's offices or storage facilities without the explicit and written permission of Sasria's Executive Manager responsible for records management acting in consultation with the Managing Director.
- (c) No Sasria staff member shall provide information and records that are not in the public domain to the public without written approval of the Managing Director as per the PAIA.
- (d) Specific guidelines for requesting information are contained in the Promotion of Access to Information Manual that is maintained by the Information Officer.
- (e) Personal information shall be maintained in terms of the Protection of Personal Information Act.
- (f) No Sasria staff shall disclose any personal information of any member of staff, client or other stakeholder of Sasria to any other person without prior written approval of the Executive Manager responsible for records management, or the Chief Information Officer as per the Information Technology policy.
- (g) Security classified documents and board reports shall be protected against or from unauthorised disclosure.
- (h) Records storage area shall at all times be protected from or against unauthorised access. In this regard the following measures shall apply:
 - i. Records storage areas and records storage facilities shall be locked when not in use.

- ii. Access to server rooms and storage areas for electronic records media shall be managed through appropriate access control authorised by the Chief Information Officer as per the Information Technology policy.

11. Managing email records

- a) E-mails that are evidence of the business transactions of Sasria are public records and shall be managed and kept for as long as they are required for functional and/or historical purposes.
- b) E-mails that approve an action, authorise 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.

12. Email of departing staff members

- a) Staff are required to perform a clean-up of all non-business related email messages in the email system prior to separating from Sasria or transferring to another organisation.
- b) The records management function in collaboration with the Human Resources department, applies clearance procedures to all staff resigning from Sasria to ensure that records and emails are identified and filed so that they can be searched for, retrieved and retained for as long as needed.

13. Clean desk practices

The following principles govern and support Sasria's clean desk practices:

- (a) Filing / Safekeeping / locking up of confidential information and documents when unattended.
- (b) Approval of clean desk procedures and processes by the relevant Executive Manager, and implementation thereof by Sasria Management and staff.
- (c) Availability of lockable storage and shredding facilities for use by all employees.
- (d) Identification, assessment and management of data and information security risks.
- (e) Monitoring of compliance with the Policy and reporting of areas of concern and / or non – compliance.
- (f) Minimising the printing of hard copy documents and encouraging the use of electronic documentation alternatives.
- (g) Reporting of incidents and information security near misses.
- (h) Training of staff to ensure awareness on the Policy and its attendant procedures and processes.
- (i) Implementing safe disposal methods for documents containing company, customer, staff and supplier sensitive and personal information.
- (j) Proper operation and security practices relating to information technology devices including computers, laptops, I-pads, cellular phones, memory sticks and other. This

- (k) includes security of data stored in the software, locking the computers off when one is not in the office or at his or her desk, and switching off of computers at the end of the work day.
- (l) Implementation of internal controls by Management to ensure that such controls are operating effectively to deter, and detect areas of, non – compliance with the Policy.
- (m) All staff being alert and actively participating in proper document and information management and security.
- (n) All persons are responsible to ensure that no Sasria documents are left behind at meeting, conference and other related venues.

14. Disposal of records

- (a) No Sasria records (including e-mail) may be destroyed, erased or otherwise disposed of without prior written request to the Executive Manager responsible for records management.
- (b) Retention periods indicated in the File Plan and retention schedule of records other than correspondence are determined taking into account Sasria's legal and functional obligations.
- (c) All destruction of records must be approved by the Executive Manager responsible for records management to ensure that archival records are not inadvertently destroyed.
- (d) Non-archival records which are needed for purposes of litigation, promotion of administrative justice actions and promotion of access to information purposes may not be disposed of until such time that the Executive Manager responsible for records Management, in consultation with Legal Department, have indicated in writing that the destruction hold can be lifted.

15. Version Control (Detailed guidance on version control will be included in the procedures)

- a) Executive Managers or their staff shall ensure version control of documents. This shall be achieved by clearly indicating version numbers on documents and by
- b) Ensuring that the latest version of a document is in use.
- c) In respect of correspondence and reports, Executive Managers or their delegates shall be responsible to ensure that copies of the approved and signed versions are archived, both in hardcopy (paper-based) and electronically (scanned).
- d) Validating performance information against the targets contained in the Annual Performance Plan (Strategic Plan) is archived and readily accessible for both internal and external audit purposes.

16. Retention Schedule

A Retention Schedule should be developed for Sasria's records by the Records Manager, and retention periods should be set in line with the National Archives and Records Service Act.

17. Key monitoring controls

The following monitoring control questions should be completed quarterly at Department level to monitor compliance:

- a) Do all documents and records created within each department have file plan reference numbers?
- b) Are records placed in the Sasria-approved file covers and filed centrally within each department and transferred to the storage area as per the retention schedule?
- c) Is the register of files opened for the department kept updated?
- d) Do staff within the department clear their workstations, scanners, shredders and printers of documents before going home?
- e) Are documents and records protected against unauthorised access, fire, water damage and dust?
- f) Has there been any request for information in terms of PAIA or PoPI recorded?
- g) Was the department able to provide the requested information within the prescribed time frame?

18. Roles and Responsibilities

Appropriate governance bodies within Sasria shall oversee the application of the information and records management risk and related policies, principles and procedures. These will be in line with among others, the Delegation of Authority Policy.

19. Applicability to employees

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

Employees of Sasria 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 Sasria will face severe court sanctions and/or a criminal charge.

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

20. Delegations of Authority

No deviation from this policy will be allowed without written authorisation of the information officer (MD).

21. Failure to Apply or Comply with the Policy

Sasria views its Information and Records Management Policy in a serious light and failure by any employee to adhere to this policy constitutes misconduct and may result in disciplinary action being taken against such employee in accordance with Sasria's Human Capital policies, as amended from time-to-time.

22. Revision of the policy

- The policy will be reviewed at three year intervals to ensure its relevance and alignment with applicable legal and governance requirements.
- Where relevant however policies may be reviewed earlier than the above three year period where there are major changes and / or gaps identified in the policy or where a shorter policy review period is dictated by law or other form of regulation.