SAICA DIFFERENCE MAKERS™

SAICA GROUP
Data & Information Governance Policy

Document control

Managed by	Risk & Compliance
Policy Owner	Executive: Risk & Compliance
Policy Sponsor (if different from owner)	Chief Operating Officer
Final approval by ExCo	7 August 2023
Next review date	6 August 2026
Version	1.0
Status	Approved

Contents

1. Introduction & Purpose

1.1. 'Information Governance' can be defined as follows: *"A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."*[1]

1.2. The SAICA Board (the Board) must govern[2] information in a manner that supports SAICA in setting and achieving its strategic objectives, and management must implement and executive effective information management.[3]

1.3. SAICA recognises information as a critical part of SAICA's operations. Information is an asset, specifically a strategic asset, and a distinct source of value creation which presents unique risks and opportunities.[4]

1.4. The Board monitors SAICA's compliance with applicable laws and non-binding rules and standards (including laws and non-binding rules and standards relating to information) with reference not only to the

[1] https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/
[2] The Board as the custodian of corporate governance within SAICA prepared the Board Charter (which is subject to the provisions of the SAICA Constitution and By-laws) in accordance with the principles of the King IV Report on Corporate Governance for South Africa (2016) (King IV).[2]
[3] Principle 12 of King IV.
[4] King IV page 34 'Technology and Information'.

obligations they create but also to the rights and protections they afford.[5] The Board should further ensure that SAICA is governed effectively in accordance with corporate governance best practices.[6]

1.5. The main purpose of this Policy is to establish the key principles and a high-level framework for information governance throughout SAICA.

1.6. A consistent and sustainable approach to information governance is required to protect the confidentiality, integrity, and availability of SAICA's data.

2. Definitions

2.1. In this Policy the terms set out hereunder shall have the following meaning:

2.1.1. **"Access"** means the right to read, transfer or query data;

2.1.2. **"Authentication"** means the process of verifying one's digital identity;

2.1.3. **"Authorisation"** means the granting of access to SAICA resources, including Institutional Information, only to those who are authorised to use such;

2.1.4. **"Authorised Agent"** means an individual or entity who is authorised by SAICA to act as its agent in specific instances and with whom an agreement has been entered into, which may include but are not limited to: Training Office Reviewers, Statisticians, independent contractors, service providers etc.;

2.1.5. **"Confidentiality"** means the preserving of authorised restrictions on information access and disclosure, including protection of personal privacy and proprietary information;

2.1.6. **"Controlled Entities"** means those Entities that are controlled by SAICA, i.e., Thuthuka Education Upliftment Fund, SAICA Enterprise Development and The Hope Factory and any other legal entity that may from time to time be established and controlled by SAICA;

2.1.7. **"Data"** means simple facts, characters, numbers, text, words, or figures which form part of information, and means little or nothing without being combined and read in contexts with other data within SAICA's possession or under its control;

2.1.8. **"Data Life Cycle"** means the process of planning, creating, managing, storing, implementing, protecting, improving, and disposing of all institutional information within SAICA, consistent with the General Data Protection and Retention Policy, Privacy Policy and the Information Security Policy and standards

2.1.9. **"Data and Information Breach"** means any security incident in which unauthorised persons gain access to or acquire sensitive or confidential Data and/or Information, including personal information;

2.1.10. **"Data Inventory Register/Data Register"** means one or more mandatory records that ensure that SAICA understands the high-level Data Sets within its data landscape along with their locations and format;

2.1.11. **"Data Set"** means a collection of actual data which are discrete items of related data that may be accessed individually or in combination or managed as a whole entity, for example business data which may include names, contact information and so forth;

2.1.12. **"Data Sharing Agreement"** outlines the framework for the sharing of data between SAICA and a third party. It defines the principles and procedures that both SAICA and the third party will both adhere to and the responsibilities on both SAICA and the third party;

2.1.13. **"Data Steering Group"** or the **"DSG"** means a working group established by SAICA Management Committee and consisting of members as set out in the terms of reference;

2.1.14. **"Documented Information Guideline"** means the process of sorting and classifying Data Sets into various types, forms, or any other distinct class, which would indicate the level of confidentiality of such a Data Set;

2.1.15. **"Employee"** means a person, excluding an independent contractor, who works for SAICA or its Controlled Entities and who receives, or is entitled to receive, any remuneration, and any other person who in any manner assists in carrying on or conducting the business of SAICA or its Controlled Entities;

2.1.16. **"ExCo"** means SAICA's Management Executive Committee;

2.1.17. **"Information"** means data which becomes meaningful and useful when processed, interpreted, organised, structured, or presented, including Personal Information and IP;

2.1.18. **"Institutional Information"** means all SAICA's information assets which can be classified into discreet categories as mandated in the Documented Information Guide;

2.1.19. **"Integrity/Data Integrity"** means the accuracy, consistency, and completeness of data over its entire Data Life Cycle, and guarding against the improper modification or destruction of information, and ensure non-repudiation and authenticity;

2.1.20. **"Intellectual Property"** or **"IP"** includes, without limitation, Designs, Patents, rights in and to Inventions, rights in and to Copyright and related rights, Trademarks, trade names and Domain Names, trade dress, rights in get-up, rights in goodwill, rights to sue for passing off, rights in designs, rights in computer software (source or object code), database rights, rights in confidential information, including Know-how and Trade Secrets, goodwill and any other IP rights, in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewals or extensions of, such rights and all

similar or equivalent rights or forms of protection which may now or in the future subsist in any part of the world;

2.1.21. **"Personal Information"** means Personal Information and Special Personal Information as defined in section 1 and 26 of the Protection of Personal Information Act, 4 of 2013, and any other applicable data governance and protection legislation, regulations, standards etc.;

2.1.22. **"Processing"** means the operation or activity or any set of operations whether or not by automatic means, concerning information, including:

2.1.22.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alternation, consultation, or use;

2.1.22.2. dissemination by means of transmission, distribution or making available in any other form; or

2.1.22.3. merging, linking, as well as restriction, degradation, erasure, or destruction of information;

2.1.23. **"SAICA"** means the South African Institute of Chartered Accountants; and

2.1.24. **"Security/Data Security"** means the protection of SAICA's data in relation to the following criteria:

2.1.24.1. access control;

2.1.24.2. authentication;

2.1.24.3. effective incident detection, reporting and solution;

2.1.24.4. physical and environmental security; and

2.1.24.5. change management and version control.

3. Scope & Application

3.1. This Policy applies to SAICA, all its activities and operations, employees, and authorised agents.

3.2. This Policy applies to, but is not limited to, all SAICA data in any form, including print, electronic, audio-visual, backup, and archived data, throughout SAICA and its entities business operations and functions.

3.3. This Policy applies to all SAICA records in all formats, including but not limited to paper, digital or audio-visual, whether in the form of files, working papers, electronic documents, emails, online transactions, data held on databases, plans, photographs, sound, and video recordings.

3.4. This Policy further applies to all SAICA Controlled Entities, all its activities and operations, employees, and authorised agents to the extent that a SAICA Controlled Entity has adopted a similar policy.

4. Policy Statement

4.1. Because SAICA is committed to govern institutional information in an ethical and responsible manner, and ensure compliance with all applicable laws, non-binding rules and standards relating to information whilst doing so. SAICA adopted the following Policy Statements:

4.1.1. **Policy Statement 1: Accountability -** Data and Information shall be managed responsibly by those who are creating, using, managing data, and those maintaining standards and compliance.

4.1.2. **Policy Statement 2: Standardisation –** Data and Information shall be uniformly structured for ease of processing and analysis by users.

4.1.3. **Policy Statement 3: Transparency** – Data and Information shall be processed in a transparent manner, and records of such processing shall be kept for the prescribed period.

4.1.4. **Policy Statement 4: Ethics** – Data and Information shall be processed in an ethical manner, which includes open dialogue about factors, limitations, choices, and consequences related to data decisions.

4.1.5. **Policy Statement 5: Integrity** – Data and Information shall be managed as a key asset by prioritising data and information quality.

4.1.6. **Policy Statement 6: Protection –** Measures shall be implemented to guard against Data and Information breaches, corruption, and losses of institutional information.

4.1.7. **Policy Statement 7: Compliance** – Measures shall be put in place to ensure compliance with applicable obligations (laws, regulations, standards, guidelines, and SAICA's policies) relating to Data and Information.

4.1.8. **Policy Statement 8: Availability** – Data and Information shall be maintained in a manner that is easy to access when needed.

4.1.9. **Policy Statement 9: Retention** - Data and Information shall be retained for an appropriate purpose and period, considering applicable obligations (e.g., laws, regulations, standards, guidelines, and SAICA's policies).

4.1.10. **Policy Statement 10: Dissemination and Deletion** – Transmission, distribution, erasure or destruction of Data and Information shall be done securely, and in accordance with applicable laws, regulations, standards, guidelines, and SAICA's policies.

4.1.11. **Policy Statement 11: Auditability -** SAICA shall maintain a Data Inventory Register to track all Data and Information to ensure that SAICA have a well-organised understanding of its data landscape.

5. Roles & Responsibilities

5.1. SAICA recognises that effective and efficient data governance is dependent on the clear assignment of accountabilities for institutional information and such information must be actively managed throughout the Data Life Cycle, through the DSG, Data Stewards, Data Manager, and Data Users:

5.1.1. **Data Ownership**

5.1.1.1. SAICA, rather than any individual or organisational unit, is the ultimate owner of all data within their area of responsibility and as delegated to them.

5.1.1.2. A Data Owner, being each SAICA Executive shall maintain ownership of and be responsible for data that originated from within their area of responsibility. The Data Owner shall be accountable for data governance outcomes.

5.1.1.3. The Data Owner shall nominate and appoint one or more Data Steward/s, as necessary.

5.1.2. **ExCo**

5.1.2.1. Shall establish a Data Steering Group.

5.1.3. **Data Steering Group**

5.1.3.1. primary goal of the DSG shall be to communicate the value of data governance internally to business users and leadership, and to assess the current state of data governance within the business organisational units.

5.1.3.2. shall be responsible for approving the procedures related to the Data Governance Policy and will also ensure that appropriate data processes are used in all SAICA's data-driven decisions;

5.1.3.3. shall be responsible for the overall management of SAICA's information governance;

5.1.3.4. establish a clear chain of custody and key data-related responsibilities throughout the organisation; and

5.1.3.5. define management of the assigned Data Set within the scope of legal and regulatory obligations.

5.1.4. **Data Steward**

5.1.4.1. Data Stewards being the employees designated to take responsibility over a data area in terms of the quality and integrity of such data, and the implementation and enforcement of data management within their Divisions, shall;

5.1.4.2. assist the Data Owner with their data governance outcomes;

5.1.4.3. be responsible for the data governance tasks required to achieve the data governance outcomes;

5.1.4.4. maintain a Data Inventory which sets out the Data Sets of the Data Owner including the determined retention period of the data in accordance with the Retention Schedule;

5.1.4.5. manage access (including authorisation) to its data and limit the sharing of information or processing of information on behalf of a third party and vice versa when a written Data Sharing Agreement or other relevant agreement is in place and subject to relevant laws, regulations, standards, and guidelines;

5.1.4.6. Protect institutional information that is stored in an electronic format and hardcopy through appropriate electronic safeguards and/or physical access controls that restrict access only to authorised users(s). Similarly, data in hard copy format must also be stored in a manner that will restrict access only to authorised user(s). Access to data in either format mentioned above must be properly tracked, logged,

and monitored, and additional security mechanisms' must be implemented, for i.e., the capability to print documents, convert documents to other formats, saving to external hard drives and uploading to clouds;

5.1.4.7. perform due diligence to ensure that the data originating from the source documents is current, complete, and accurate on the relevant information systems;

5.1.4.8. be responsible to ensure that data processed classified in accordance with the Documented Information Guideline and processed is in accordance with all SAICA policies and procedures, and applicable, laws, regulations, standards, and guidelines;

5.1.4.9. be responsible for the quality and integrity, implementation, and enforcement of data management within their organisational unit. The Data Steward understands SAICA's requirements for collecting and holding data, including its permitted uses, processing, and disposal;

5.1.4.10. ensure that the requirements of the Data Governance Policy and Procedures are followed within their organisational unit, and therefore requires access to Information Technology support tools to allow viewing and monitoring of data within their organisational unit; and

5.1.4.11. ensure that an Data Protection Impact Assessment (DPIA) is performed in the event in which the Data Owner is planning to process Personal Information in particular with new technologies, taking into account the nature, scope, context and purposes of processing, is likely to result in high risk to the rights and freedoms of individuals and/or juristic persons SAICA and/or its Controlled Entities shall prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Information. A single assessment may address a set of similar processing operations that present similar high risks.[1] The DPIA must be performed in accordance with the DPIA Procedure.

5.1.5. **Data Manager**

Shall be the Project Manager: Information Governance & Protection / Information Officer situated in the Ethics & Compliance Department, Risk & Compliance. The Data Manager's main role is to support and advised SAICA business on how to manage its data including, defining, and implementing data migration strategies and Data Policy frameworks in line with SAICA business and project data requirements;

5.1.5.1. Shall manage SAICA's legal risk in terms of Information Governance & Protection. Shall develop and implement an Information Governance Framework which provides for a logical structure for organising how SAICA deals with and communicate data governance concepts and principles regarding institutional data.

5.1.5.2. Provide support services to Data Owners, Data Stewards, and Data Users on how to manage its data, including defining and implementing data migration strategies and data policy frameworks in line with SAICA's data project requirements.

5.1.5.3. Perform the Information Officer duties in accordance with POPI and other related data protection laws, regulations, standards, guidance etc.

5.1.5.4. Establish a Data Inventory and maintain same.

5.1.6. **Data Users and Authorised Agents**

"Data User/s" and "Authorised Agents" refer to any SAICA employee or SAICA authorised agent, with varying access rights, who accesses, inputs, amends, deletes, extracts, and analyses data to carry out their day-to-day duties; but are not usually Data Stewards or Data Managers;

5.1.6.1. Data Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access.

5.1.6.2. In some instances, the same person may perform dual roles as a Data User and Data Steward.

5.1.6.3. Any errors found in the data housed in any system shall be reported to the relevant Data Owner Division.

5.1.6.4. At all times adhere to all appropriate data security measures to ensure safety, quality, and integrity of institutional data.

5.1.7. **Information Technology Department & Facilities Services Management**

5.1.7.1. Provide support services to Data Owners by providing technological tools (including data systems, data security tools, authentication, and physical security tools) necessary to process data securely.

6. Reporting

6.1. This Policy imposes a duty on all persons to whom this Policy or the principles thereof apply to report non-compliance to this Policy to the Policy Owner. Alternatively, must report such via SAICA's Anonymous Tip-off Hotline. Please refer to the Whistleblowing Process for guidance on how to report.

6.2. The Policy Owner shall report non-conformance to this Policy to the Ethics and Compliance Department as and when it happens monthly and provide continuous quarterly status updates on non-compliance conformance reports.

7. Remedial Action & Sanctions

It should be noted that should the employees, service providers, stakeholders and contractors fail to adhere to this Policy, such conduct may result in disciplinary action being taken in accordance with SAICA's Disciplinary Procedures and other relevant procedures.

8. Approval & Effective Date

This Policy shall be approved by ExCo and shall come into effect one month after approval by ExCo, subject to the completion of implementation and the necessary training provided and awareness created by the Policy Owner.

9. Review of Policy

9.1. This Policy will be reviewed every 3 years or as and when required, in order to ensure that the terms are current, fair, and representative of relevant corporate and industry conditions.

9.2. The Ethics & Compliance Department is responsible for maintaining and revising this, Policy.

9.3. SAICA reserves the right to change this Policy at any time, without prior notice and will communicate such changes to all affected.

POLICY SIGN-OFF AND OWNERSHIP DETAILS

Policy Title	Data & Information Governance Policy
Review Date	6 August 2026
Related Legislation Applicable	Protection of Personal Information Act, 4 of 2013, General Data Protection Regulations 679/2016 of the EU, King IV
Related Policies, Procedures, Guidelines, Standards, Frameworks	Information Retention Schedule, Data Impact Assessment Procedure, Documented Information Guideline, Personal Information Protection Guideline, Information Security Policy, Acceptable Use Policy, Access Control Policy, Remote Working Policy, Mobile Device & Teleworking Policy, Employee Social Media Policy, Public Statement (Media Statement, Advocacy and Spokesperson) Policy, IT Incident Management Policy, Asset Management Policy, Intellectual Property Policy, Corporate Identity Policy, Employee Code of Ethics
Replaces	Data Ownership Policy V1.0, General Personal Information Protection & Retention Policy V1.1, and Privacy Policy V1.1.
Policy Owner	Executive: Risk & Compliance
Policy Sponsor (if different from Policy Owner)	Chief Operating Officer
Application	SAICA and its Controlled Entities, employees, contractors, and consultants.
Functional Owners	Ethics & Compliance
Status	Approved
Final Approval by ExCo	7 August 2023
Version	1.0

Sign-off:
The following party is a signatory to the content of this policy:
Signed by the Chairman of the ExCo

_____

Chairman of the ExCo
Date: 7 August 2023

Rivision History

Version	Date	Revision Description & Summary of Changes (for audit trail purposes) **Note: The Change Risk Management process must be followed where significant changes are made to this policy.**	Policy Owner & Policy Sponsor
[2.0]	[DD:MM:YY]	[Major Revision: Legislative amendment (Approval required)	-
[1.1]	[DD:MM:YY]	[Minor Amendments: formatting (No approval required)]	-
1.0	[07:08:23]	First draft: new policy	Executive: Risk & Compliance & Chief Operating Officer

End of Policy