DATA MANAGEMENT: Governance & Management Policy

alexforbes.com

alexforbes
insight • advice • impact

TABLE OF CONTENTS

1 Introduction

1.1 Corporate Governance

1.1.1 Data Governance is an essential element of Corporate Governance, providing for the protection, design and execution of data planning and data quality needs in support of our client's needs and Alexander Forbes' strategic information requirements.

1.1.2 Data is a strategic asset maintained to support the Group's products and services as well as to ensure the financial well-being of its customers.

1.1.3 To effectively support the Group's strategic plans and innovative management of data, data must be readily accessible, complete for its intended purpose, and without duplicates.

1.1.4 Data must accurately represent the information it contains, improve the security of the data, including confidentiality and protection from loss and safeguard the rights and license in and to data, content, or intellectual property.

1.1.5 Finally, Data Governance also seeks to upheld statutory, data privacy and financial reporting requirements, as well as to facilitate the controlled integration across all information systems.

1.1.6 This policy aims to establish a control environment for data to be produced and consumed in a manner that achieves the minimum standard requirements while equally driving continuous data management and quality improvements.

2 Purpose

2.1 Data Governance

2.1.1 Information Governance is defined (see DMBOK2, 2017) as the processes, roles, methods, standards, and metrics that ensures the effective and efficient use of data in enabling an organisation to achieve its goals. In other words, Information Governance encompasses the systems (including policies, processes, and technology) by which information is controlled and secured.

2.1.2 Our first step in this governance journey is this policy to describe our adopted framework guiding the Group's data lifecycle management. This means the sequence of stages that a particular unit of data goes through, from its initial generation or capture to its eventual archival and/ or deletion.

2.1.3 This policy specifies the usage responsibilities of stakeholders and is underpinned by the following general core Data Management principles:

- Create a data management strategy.
- Define roles in the data management system.
- Control data throughout its lifecycle.
- Ensure data quality.
- Collect and analyze metadata.
- Maximize the use of data.
- Protect data access (normalized and secured via a data virtualization method).
- Allow for reusability of data models by Business Units ('BUs').
- Support the 8 conditions contained in POPIA, namely:
  - Condition 1 - Accountability
  - Condition 2 - Processing Limitation
  - Condition 3 - Purpose specification
  - Condition 4 - Further processing limitation
  - Condition 5 - Information quality
  - Condition 6 - Openness
  - Condition 7 - Security safeguards
  - Condition 8 - Data subject participation

2.1.4 Adherence to this Data Governance Policy will:

- Enhance board oversight of organizational data governance.
- Enable data management governance and control requirements in line with business (operational), legal and regulatory requirements.
- Provide implementation requirements for continuous improvement, accurate and timely data management.
- Establish appropriate accountabilities and responsibilities for the management of data as

an organizational asset amongst key stakeholders.

- Define clear roles and responsibilities for different data usage, collection, elimination and establish lines of accountability.
- Ensure that the Alexander Forbes Group complies with applicable laws, regulations, contracts, and standards and properly evidences such compliance.

3 Scope

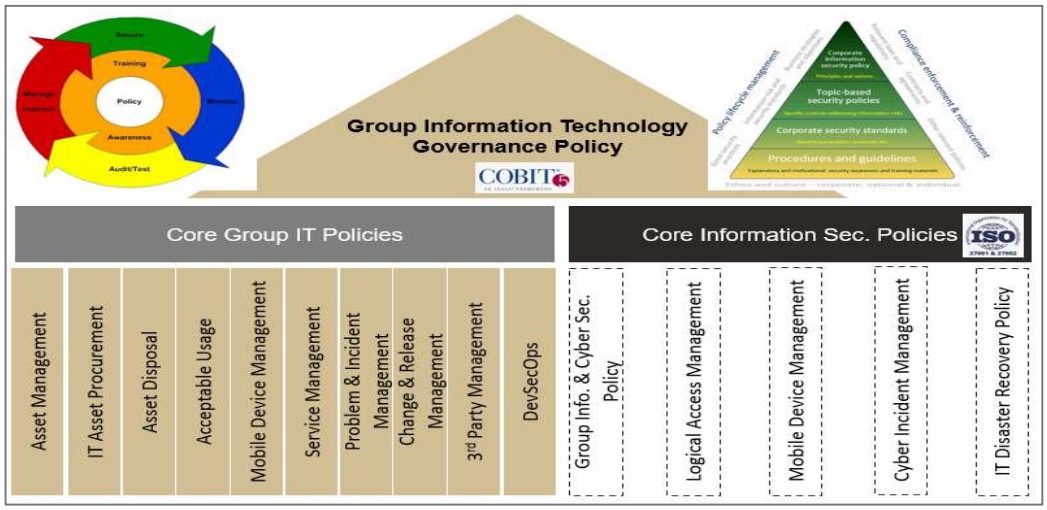
3.1 Application

3.1.1 This policy applies to all Alexander Forbes Group Holdings Limited employees and contractors as well as employees of all its subsidiaries, joint ventures, associates, and trusts, collectively ("the Group" or "Alexander Forbes") who receive, provide, create, or otherwise use data related to Alexander Forbes and its clients, regardless of the form of storage, presentation, or access.

3.1.2 The standards described in this policy sets the foundation for the minimum compliance requirements that are acceptable for good data governance practices, and further apply to anyone engaged by the - through employment or third-party contracts - who obtains, creates, manages, processes or reports on data created in any form, including but not limited to, print, electronic, audio-visual, backed up and archived data on behalf of Alexander Forbes. This will also include the Group being requested to provide data for litigation or subject to regulatory investigations and compliance objectives.

3.1.3 All senior personnel have the responsibility to understand and implement this policy, including, as necessary, the adoption of specific processes, standards, and procedures for their respective areas in furtherance of and in accordance with this policy.

3.1.4 Related policy documents - This policy should be read in conjunction with the below mentioned policies:



- AF Information Security (InfoSec) Policy and internal procedures.
- Group Technology Governance Policy.
- Records Management Policy.
- Data lifecycle & Quality Policy.
- Records Management Policy
- Data Sharing Policy
- Group Privacy Policy

4 Core Data Management Principles

4.1 Overview

4.1.1 The following principles outline the minimum standards that guide the Group's data governance practices. The core principles are:

- All Data Sources to be consumed through the Data Virtualization layer (Denodo VDP).
- Data must not be duplicated or exist outside of its data retention requirements (set by law).
- Unused data should be securely archived, and access revoked.
- When on-boarding new data sources, the inherent risks and data privacy obligations should be considered.
- Data Security Roles (ownership and stewardship) must be allocated to enable governance and stewardship.
- Data quality (DQ) / accuracy methods should be adopted by business and facilitated by the Data Governance team and data stewards
- Data sharing must be approved by nominated data owners and implemented through the Data Governance structures.

STANDARDS	CONTROL REQUIREMENT
Data Governance Standards	▪ Data Governance organisational structures, roles, responsibilities, and controls must be implemented at Group level and BUs. ▪ All BUs are required to formalise accountability for data governance activities.
Metadata Management Standards	▪ Controls must be implemented to identify, activate, and manage data domains, to identify critical data elements (CDE's) and to define and manage management activities.
Data Quality Management Standards	▪ Controls must be implemented to effectively manage the quality of data and thus ensuring that its application is appropriate and accurate for purpose.
Data Lineage Standards	▪ Controls must be implemented to capture and harvest data lineages and to enable the establishment of appropriate data quality and integrity controls during transmission from source to target (end-to-end).
Data Architecture Standards	▪ Controls must be implemented to define and implement a data architecture across the Group that is adaptable to meet business requirements. ▪ Controls must be implemented to manage the adoption of authoritative data sources, including processes for provision and consumption.
Master and ReferenceData Management Standards	▪ Controls must be implemented to manage an enterprise reference data master register for the Group's data domains.
Data Lakes and Warehousing Standards	▪ Controls must be implemented to manage the organisation of a data lake environment, aggregated data repositories and capabilities.

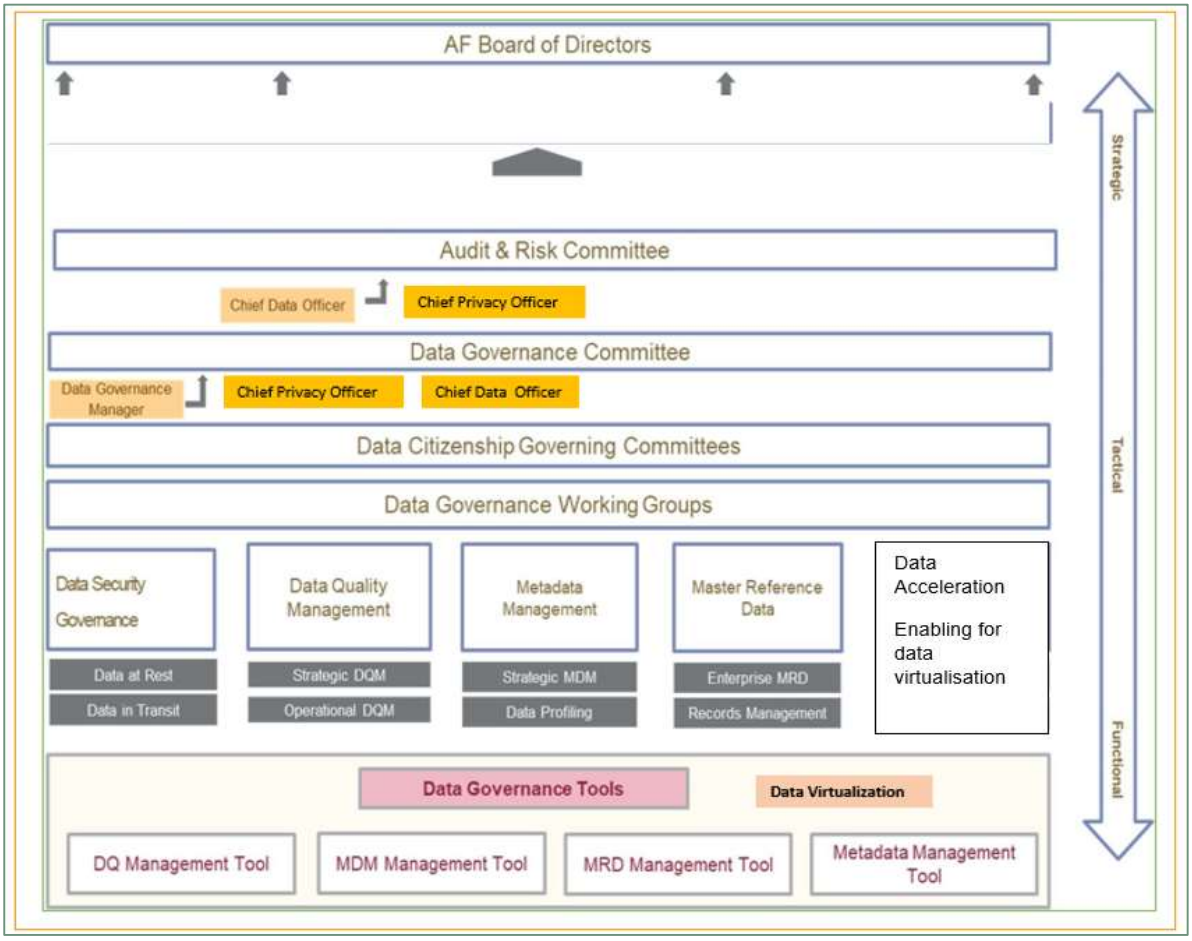
STANDARDS	CONTROL REQUIREMENT
3rd. Party Data Standards	▪ Controls must be in implemented to manage the standards for sharing data with 3rd party partners and data operators. Typically achieved by way of adopting a Service Level Agreement and / or Data Sharing Processing Agreement.
Business Intelligence Standards	▪ Controls must be implemented to ensure an effective business intelligence capability that provides trusted and valuable insights about the Alexander Forbes business and customers. ▪ These includes capabilities such as Management Information, Data Analytics, Advanced Analytics, Data Science and Artificial Intelligence.

4.2 Data Control Requirements

4.2.1 Data must be governed and managed in accordance with applicable legal (global and local), statutory and regulatory requirements where these exceed requirements set in this policy. Any additional jurisdictional requirements must be adhered to in addition to the requirements outlined in this policy.

4.3 Data Governance and Structures

4.3.1 A three-level structure accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archiving and destruction of information – Data Governance – is depicted in the following diagram as illustrated.



4.3.2 Responsibility for the activities of data governance is shared among the roles listed. Descriptions of roles and responsibilities below provide the framework of how data governance will be implemented and maintained.

4.3.3 A Data Governance Committee is established to set and drive through policy compliance as well as act as the decision-making authority regarding data management practices within the Group.

4.3.4 The Data Governance Committee will review and support proactive as well as reactive change management activities in support of data management initiatives. This includes the implementation of group-wide meta-data, data quality, reference and master data solutions to enable accurate and timely data management practices.

4.4 Data Governance Structures Roles & Responsibilities

COMMITTEE	ACTIVITIES
Data Governance Committee (Strategic)	▪ Provide strategic direction, ensuring that data governance efforts address all relevant and mission-critical needs of the Group. ▪ Manages data governance as an integrated program. ▪ Sponsors approve and champion the governance goals. ▪ Reports back to supervisory structures periodically. ▪ Address and resolve escalated issues. ▪ Approves policies, processes and tools and ratify standards to meet governance goals.
Data Citizenship Governing Committees (Strategic/Tactical)	▪ Carry out plans and policies to implement with guidance from the Data Governance committee, including: o Creates and approves policies, processes and tools and define standards to meet governance goals. o May initiate or select tools, policies, and processes. o Address and resolve issues escalated to this level. o Chair data related workgroups. o Meet regularly to address data issues. o Reports back to relevant management structures periodically. o Attend to the management (registration and tracking of) data extraction and integration procedures (ETL, data virtualization or otherwise) via the data CoE team
Data Governance Working Groups (Operational)	▪ Implement plans and policies developed by the Data Governance Committee including: o Analyse and resolve any data problems that arise. o Lead and organise workgroups for addressing continuous improvement projects o Conduct data training. o Suggest policies, business rules and processes to the Data Governance Committee. o Participate in tool selection processes

COMMITTEE	ACTIVITIES
	○ Communicate concerns, issues, and problems with data to the individuals who can influence change

4.4.1 The Data Management Office will facilitate and co-ordinate activities of the committee, councils, and data stewardship. It will engage a variety of stakeholders in support of company-wide data governance and management including the creating and operationalization of applicable standard operating procedures ('SOPs') and practices.

4.4.2 The Data Management Office is responsible for developing plans to capture and record specific data administration-focused meta-data consistently with a defined meta-data program.

4.4.3 Data Stewardship practices will be established at a BU level as part of the formation of the Data Governance Committee to align and co-ordinate data architecture activities, monitor and remediate data management issue escalations and enforce standards.

4.4.4 As part of Data Management Councils, the business SMEs, stewards, and data owners are expected to play an integral role in the detection and resolution of data related issues.

4.4.5 Data management and stewardship processes must exhibit transparency; it should be clear to all participants and auditors how and when data-related decisions and controls are implemented.

4.4.6 These participants should also ensure that a data audit trail is effectively documented within the processes associated with accessing, retrieving, reporting, managing, and storing of data.

4.4.7 All participants are expected to practice integrity in their dealings with each other; they will be truthful and forthcoming when discussing drivers, constraints, options, and impacts for data-related decisions

4.5 Roles and responsibilities of stakeholders

4.5.1 Group Information Officer

- Approve requests for information under the PAIA (Promotion of Access to Information Act) alongside Data Owners.
- Ensure, guide, and help influence business to meet legal compliance in respect of POPIA.
- Ensuring that developments in the statutory and regulatory environments are communicated to all data governance / management managers, and that the implications of such developments are understood and mitigated for.
- Issue data destruction certificate as part of the data destruction process in consultation with our Chief Data Officer.

4.5.2 Chief Data Officer

- Accountable for Data Governance within the Group.
- Guide and influence Data Governance operational compliance and communication within the Group

- Manage the Data Governance team and Data Virtualization platform (DENODO)
- Overall responsible for DQ initiatives and delivery.
- Issue data destruction certificate as part of the data destruction process in consultation with our Group Privacy Office.

4.5.3 Business Managers (Data Owners)

- Ensure that data generated, stored, archived accurately and disposal references are procedurally updated.
- Ensures the classification and reclassification standards are adhered to.
- Monitor procedural amendment of authorized content; escalate report unauthorized edits.
- Ensures accuracy of published content, documents, and records.
- Implementation of the policy in their respective teams.
- Ensures staff are aware of their Data Governance responsibilities and obligations in terms of the policy.
- Manage 3rd party agreements for off-site physical data storage/destruction (with Procurement).

4.5.4 Data Governance Manager

- Ensures that all policies and procedures defined for Data Governance are current, relevant and updated.
- Drives the data governance strategy along with Executives, business, and our data stewards.
- Ensures that all activities of the various Data Governance units are coordinated and in alignment.
- Resolve contradictions between policies and processes.
- Execute on the delivery of data virtualization and DQ data quality initiatives.

4.5.5 IT Managers

- Support the Data Owners by advising on and ensuring the provision and maintenance of appropriate infrastructure for the proper management of this policy.
- Ensure the security of digital/electronic contents, document, and records.
- Assist with the day-to-day maintenance of electronic systems of storage and backups.
- Advise management regarding appropriate storage, archival and disposal strategies for unstructured data.
- Ensure controlled accessibility of data on IT systems by ensuring that adequate plans are in place for protection, backup, and disaster recovery.
- Provide regular reporting to various management levels throughout the lifecycle of content, documents, and records.

4.5.6 Data Stewards

- Data stewards are accountable for the management of all data within and used by their respective BU's and ensuring that the data-related rules as established by the data governance program are followed.
- Perform Data Governance implementation duties in relation to content and document management procedures as required by the Data Governance related policies and standards.
- Assist BUs in operationalizing strategic plans for data warehousing, processing, and reporting.
- Determining and ensuring compliance to all Data Governance and Management policies and standards.
- Ensure compliance to Data Governance principles, policies, and standards to ensure that data is effectively governed.
- Administer the rollout of Data Governance principles to all business teams and manage work as a single point of contact.
- Providing support to business processes in maintaining data and managing it according to data properties as required by administration.
- Administration of efficient processes to capture and maintain data governance principles (Metadata, data quality (DQ) and data lineage).
- Coordinate with stakeholders (technology and business) to provide all definition for critical data elements.

4.5.7 Operational Data Management

- All staff, management and stakeholders must recognise the core principles set out in this policy.
- Individuals designated as data stewards will have specific accountabilities (such as data definition, data production and data usage) incorporated into their functions.
- Group data is to be modelled, named, and referenced in a uniform way by choosing data virtualization methods and software.
- Enterprise data and the meta-data about that data are owned collectively by the BUs and managed by way of the established Data Governance structures.
- Enterprise meta-data shall be readily accessible, except where it is determined to be restricted for security reasons. When restrictions are made, data stewards are accountable for defining specific individuals and levels of access privileges that are to be enabled.
- All Enterprise information systems development and integration projects will utilize the defined Enterprise Data Model (EDM) via the approved software program for data naming, data modelling, and logical and physical data design.
- Enterprise data in all formats shall be safeguarded and secured based on recorded and approved security and compliance requirements. These requirements are to be determined by the data stewards working within the council.

- Subject to data privacy and protection, every effort must be made to share data across the Group and not to maintain redundant data without justification.
- Data owners must recognize and support the data/informational needs of up and downstream processes and business units that may require said data.
- Data quality standards shall be managed and applied actively by all stewards to ensure a reliable level of Enterprise Data as defined by the data management councils.
- Appropriate backups and disaster recovery measures shall be consistently implemented, administered, and deployed for all Enterprise Data.

4.6 Data Classification

4.6.1 The following outline the minimum standards guiding the Group's data classification processes at a high level (see "Data lifecycle & quality policy):

4.6.2 Classification of datasets and data outputs is done by assessing the cross-section of regulatory risks and business risks and determining the net impact from both dimensions if there were to be a breach. Alexander Forbes data to be categorized into one of four classifications. They are:

- **Confidential,**
- **Sensitive,**
- **Internal and**
- **Public** (see Information Security Policy).

4.6.3 During the creation of data, it should be classified and treated at the appropriate level of data security and protection.

4.6.4 During data usage, ongoing re-evaluation of data classification should be conducted and when necessary, data should be re-classified.

4.6.5 Data owners are accountable (delegated from the data owner) for labelling data with an appropriate "information sensitivity" classification prior to distribution.

4.7 Data Privacy and Protection

4.7.1 Data privacy or information privacy is a branch of data security concerned with the proper handling of data - consent, notice, and regulatory obligations –

> (Note - please read this together with the Group Privacy Policy, as hosted on the Policy Passport portal - *https://aforbes.policypassport.com/assignments/c34d3fcd94*

4.7.2 More specifically, practical data privacy concerns often revolve around:

- Whether or how data is shared with third parties.
- How data is legally collected or stored.
- Data Subject rights and access to their personal information processing.
- Data (access) breach notifications to the relevant stakeholders.

4.7.3 The purpose of the POPI Act is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to

justifiable limitations that are aimed at:

4.7.4 Balancing the right to privacy against other rights, particularly the right of access to information.

4.7.5 Protecting important interests, including the free flow of information within the Republic and across international borders.

4.7.6 Regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.

4.7.7 Provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act

4.7.8 POPIA sets the legally mandatory requirements for the processing of personal information into 8 objectives as also captured in our Group Privacy Policy section 4. They are:

- Condition 1 - Accountability
- Condition 2 - Processing Limitation
- Condition 3 - Purpose specification
- Condition 4 - Further processing limitation
- Condition 5 - Information quality
- Condition 6 - Openness
- Condition 7 - Security safeguards
- Condition 8 - Data subject participation

4.7.9 A privacy policy is a statement or legal document (in privacy law) that discloses some or all the way a party gathers, uses, discloses, and manages a customer or client's data. The Alexander Forbes Privacy notice reads: *https://www.alexanderforbes.co.za/download/afo/Manuals/Alexander%20Forbes%20Group%20Holdings%20Privacy%20Policy.pdf*

4.7.10 Where data contains Personal Information or Sensitive Information additional care is required to ensure appropriate treatment. Such treatment is the subject of additional policies such POPIA Policy in South Africa or equivalent policies in other territories amongst other relevant regulations as may be applicable, all of which needs to be complied with.

4.8 Data Access & Sharing

4.8.1 In line with the data classification objective, assigned access to data must be restricted to those who require it to perform their organisational duties. Such access should only be granted if the request meets a reasonable business requirement as determined by the data owner.

4.8.2 Where granted such access should not be shared with parties other than those authorised for the intended purpose.

4.8.3 Reasonable efforts should be made to ensure procedures and mechanisms established to protect data do not unduly interfere with the efficient execution of the intended purpose.

4.8.4 Prior to sharing data, all parties involved in the exchange must enter into a Data Sharing Agreement. Such agreements must be provided as record to the Data Management Office and Procurement for storage.

4.9 Data Usage

4.9.1 Authority to view (use) data shall be granted by the appropriate Data Owner (BU), at their discretion, to Data Users where their organizational duties do not specify or require them the responsibility to update data i.e., read-only.

4.9.2 Authority to update data shall only be granted by the appropriate Data Owner (BU) at their discretion to Data Users where their organizational duties specify and require them the responsibility to update data.

4.9.3 Data Users may only access and use data as required for the performance of their organisational duties, and not for other or inappropriate purpose. Data users may only use data according to the security levels assigned to their function.

4.9.4 Adequate controls and/ or management procedures will be implemented consistently to manage the usage and updating of data across the Group. Such controls may include audit logging to ensure traceability of changes applied.

4.9.5 Data Owners should determine when data de-identification is required prior to sharing for analytical or statistical purposes.

4.10 Data Integration

4.10.1 Data extraction and integration procedures (ETL, data virtualization or otherwise) should be registered and facilitated via the data CoE team.

4.10.2 Downloading of data from central systems to electronic files for the purpose of uploading or connecting the data to another system without the appropriate registration and approval is not permitted.

4.10.3 The responsible Data Management Council must ensure, as far as practicable, the accuracy, correctness and completeness of data supplied to integrating parties (internally and externally).

4.10.4 Such documented/registered data integration must be periodically maintained by the systems providing or integrating data and resubmitted to the data CoE team.

4.10.5 Where such integration supports analytical or reporting purposes, periodic data reconciliations to source must be performed and evidence maintained for an audit function (internal or external) as directed by the Data Governance Committee.

4.11 Data Integrity

4.11.1 Data Integrity must be consistently maintained throughout the data lifecycle.

4.11.2 Data users must ensure that data is captured and/ or updated accurately and as far as reasonably possible ensure input validations are implemented to prevent incorrect data

entry.

4.11.3 Appropriate levels of confidentiality and compliance with privacy laws must be maintained during the collection, use, transmission archival and destruction of data.

4.11.4 Regular self-assessments audits, by the Data Stewards to gain insights on their departmental data remediation efforts should be initiated and performed as this will aid decision making iro data quality work to be performed. on the integrity and quality of data must be performed to ensure that business and quality standards are being upheld.

4.11.5 The data CoE team to implement and execute a process for monitoring and reporting the integrity of data throughout the Group and all its information systems.

4.12 Data Retention, Archival or Destruction

4.12.1 Data usage and retention periods must be defined and communication for data sets per BU after which it must be either archived or appropriately destroyed. These periods must be consistent with legal, contractual, regulatory, and ethical obligations as documented by the BU.

4.12.2 All data that is subject to litigation or forensic discovery may be needed for legal action or record and should therefore be retained and where possible archived but remain readily accessible should the need arise. If in question – Data Owners (BU) to reach the Data Management Office and the Privacy Office.

4.12.3 A central catalogue of all archived data should be controlled (maintained and updated) by the Data Management Office on an ongoing basis, preserving access control privileges. Authorised jointly by the Group Information Officer, Group IT governance head and the Data governance team.

4.12.4 All archived data needs to be stored safely for reliably with a clear process for timely retrieval (unarchiving) as and when required by the business.

4.12.5 A destruction certificate should accompany and be generated as part of the data destruction process.

4.12.6 Where appropriate data owners and data custodians should restrict the ability to alter data, process parameters, or authorised destruction of data by technical means.

4.13 Unstructured data

4.14.1 Business documents and forms relating to business process should be stored in a suitable document or/ and official management repository. Unmanaged file shares should not be used for data storage.

4.14.2 The data owner before publication must approve digital content.

4.14.3 Data Owners together with the data stewards must define and document what constitutes a record in their respective business areas. (Records form a legally binding base for action and may include both digital and paper-based data).

4.14.4 Regular data access audits should be conducted, and remediation processes put in place to ensure adequate management and controls are in place.

4.14.5 Data ownership, custodianship and stewardship should also be mapped for unstructured data; user groups and apply appropriate user access controls.

4.14 Data Analytics & Artificial Intelligence

4.14.6 Business support data analytics and artificial intelligence should only be performed off a well-maintained data warehouse or data lake that publishes reconciled data (e.g. quality or trust levels) for the data sets consumed.

4.14.7 Authoritative master records for entities must be obtained from an approved master-data and reference management source.

4.14.8 Transactional master records related to the entities must be obtained from either the originating data source or the authorised operational data store (which may include unstructured data).

4.14.9 To ensure human interpretability of artificial intelligence decisions (such as Machine Learning, Robot advice, Fraud detection, Automated Investment, etc.), records of test/control group results that have been approved prior to productive usage must be maintained and updated regularly.

4.14.10 Learning algorithms should include the generation of meta-data required to support traceability of the data used in decision-making.

4.15 Cloud Data Solutions

4.15.1 Agreements with Cloud Solution providers must include a provision under which all data relating to the Group can be recovered and removed from the cloud solution timeously and on-demand by the Group. Additional provisions must consider physical access, protection against data loss, threats to data privacy, transitions to another provider and breaches of confidentiality.

4.15.2 Compliance for cloud solutions, devices and applications must align with this policy and generate reports that are sufficiently detailed to prove the security controls are working and providing adequate evidence to allow investigation and remediation when the controls fail. Evidence of relevant control technologies that keep data identifiable, in known locations, offline backups and within the control of the Group must be provided periodically to ensure data is safe and secure as well as reliably accessible.

4.15.3 Preference should be given to direct (non-public) network connections to cloud solution provides and appropriately secured (e.g., encryption).

4.15.4 Offline data backups of cloud solutions must be included in the relevant service agreements.

4.15.5 Additional caution must be applied when data subject to privacy laws is to be stored in cloud solutions. These cases require explicit approval from the Data Governance committee and

any other appropriate body within the Group (e.g., Group Risk Committee).

4.15.6 A data disaster recovery plan should be in place to create back-up files for all datasets stored at the cloud.

4.15.7 A data disaster recovery plan should be in place to create back-up files for all datasets.

5 Responsibilities

5.1 Maintenance and Revision

5.1.1 The document owner is responsible for the reviews of their documents, aligned with the frequency as included in the document, to ensure continued relevance in governing the business activities appropriately.

5.1.2 This policy is enforced and maintained by the Data Governance committee (Chaired by the Chief Data Officer), and operationalized in collaboration with relevant Data Governance Structures, IT and/ or BU departments and other business functions such as Governance Legal & Compliance, Internal Audit, Risk and Procurement which must always be consulted when making changes to this document.

5.1.3 Our Data Governance committee and Group Data Information Officer is accountable for the policy implementation and business execution.

5.1.4 Behaving in a manner contrary to what is contained in the policy will constitute a violation or breach of the policy which may be referred to relevant disciplinary processes

STRUCTURE / FUNCTION	ROLE	INTEREST, DUTIES & RESPONSIBILITIES
Accountable Business Units	**Business Record Owners** (Business Managers/Heads)	▪ Ensures the effective implementation of the document and records management system. ▪ Ensures that appropriate resources are provided for the management of documents and records. ▪ Ensures information, training and instruction is provided on the document and records management system. ▪ Reviews and provides final approval of all relevant documentation.
Accountable Business Units	**Business Records Controller** Data Steward (Business Analyst)	▪ Ensures that documents and records archive and disposal references are procedurally updated. ▪ Ensure the classification, reclassification and handling of documents and records. ▪ Ensure staff are aware of their responsibilities and obligations in terms of the policy. ▪ Manage third party agreements for off-site physical data storage/destruction (with Procurement). ▪ Ensuring documents are developed using correct styles and format. ▪ Maintaining the document register. ▪ Archiving of all obsolete documents and records.
Governance & Compliance	**Records Governance Lead** Data Governance Manager	▪ Ensures that all policies and procedures defined for data governance are current, relevant, and updated. ▪ Drive the records management strategy along with the Group Information Officer and Chief Data Officer. ▪ Ensure that all activities of the various data governance units are coordinated and in alignment. ▪ Provides direction on the records taxonomy; classification system; indexing; metadata management ▪ Resolve contradictions between policies and processes.

STRUCTURE / FUNCTION	ROLE	INTEREST, DUTIES & RESPONSIBILITIES
Governance & Compliance	**Records Governance Analysis** Data Governance Analysts	▪ Work closely with the Data Governance manager in ensuring that: o All policies and procedures defined for data governance are current, relevant, and updated. o Drive the records management strategy along with the Chief Data Officer. o All activities of the various data governance units are coordinated and in alignment. o Contradictions between policies and processes are resolved.
Accountable Business Units	**Document & Records Manager** **Enterprise Content (ECM) Manager**	▪ Definition of detailed procedures for the creation, authorization, publication and management of AF Documents and records management, on all platforms including digital. ▪ Develop practical plans for the implementation of this policy in Alexander Forbes Group. ▪ Review and maintain the content and document policy documents.
Accountable Business Units	**IT/Application Managers**	▪ Support the Documents and Records Management Manager by advising on and ensuring the provision and maintenance of appropriate infrastructure for the proper management of this policy. ▪ Ensure the security of digital/electronic contents, document, and records. ▪ Assist with the day-to-day maintenance of electronic systems of storage. ▪ Advise management regarding appropriate storage, archival and disposal strategies for unstructured data as per the information security and records policy.
Governance & Compliance	**Governance Legal & Compliance & First Line Compliance**	▪ Ensure that developments in the statutory and regulatory environments are communicated to all data governance / management managers, and that the implications of such developments are understood and mitigated for.

5.2 Legal Accountability & Admissibility

5.2.1 This policy is subject to the legislative and regulatory frameworks of the Republic of South Africa and in-country laws in international territories where Alexander Forbes has a footprint. It is informed by requirements from the Legislative Universe as published on the AF Intranet and considers related leading accepted industry good practices.

5.2.2 It should be noted that electronic data is considered admissible in legal actions and that the relevance of related data may need to be demonstrated also (e.g., electronic documents, email or database records).

5.2.3 Unauthorised removal or destruction of data from Alexander Forbes' systems, databases and premises could be seen as circumvention or evasion and must therefore clearly follow the governance and management practices set out in this policy. This is aimed at ensuring their authenticity, that they are unaltered, auditable, and secure.

5.2.4 Legal accountability or liability for decisions taken based on data must always be clarified, especially when human agency is replaced by means of artificial intelligence.

5.3 Monitoring and Review

5.3.1 The implementation, application, and relevance of the principles of this policy must be monitored and reviewed regularly by the Group Information Officer and Chief Data Officer or any designated official and all key Business Units (BU).

5.3.2 The Data Governance committee should ideally (annually) commission an independent audit of the Data practices arising from this policy. A detailed review of the audit findings must be discussed at a sitting of the committee within six (6) weeks of submission of the final audit report. The resolutions of the meeting must be documented, communicated, and filed.

5.3.3 The Chief Data Officer must ensure that the findings of the audit and resolutions of the committee are, where appropriate, considered in policy, process, procedure, project, and strategy reviews to ensure that Data practices in Alexander Forbes remain relevant, efficient, and effective.

5.4 Training and Awareness

5.4.1 Alexander Forbes Executive management is accountable for the implementation of this policy within their departments and business units. The roles and responsibilities are outlined in the Governance committee and should be signed-off by all mandated stakeholders.

5.4.2 Each data environment within the Group must have a training plan for the various categories of users it services, and for the development of the technical team. All senior resources must be, or have a plan to be, certified in data management practices that are relevant or complementary to their roles and development goals.

5.4.3 The DMO must develop communication strategies to widely communicate the requirements and obligations of this policy. The DMO must further ensure that the roles and authorities required to implement this policy are clarified and assigned; and that appropriate training is identified and developed / sourced.

5.5 Policy Governance

5.5.1 The Document Owner is responsible for the reviews of their documents, aligned with the frequency as included in the document, to ensure continued relevance in governing the business activities appropriately.

5.5.2 This policy is enforced and maintained by the Data Governance Committee (Chaired by the Chief Data Officer), and operationalized in collaboration with relevant Data Governance Structures, IT and/ or BU departments and other business functions such as Legal, Audit, Risk & Compliance and Procurement which must always be consulted when making changes to this document.

5.5.3 Our Data Governance Committee and Group Information Officer is accountable for the policy implementation and business execution.

5.5.4 Behaving in a manner contrary to what is contained in the policy may constitute a policy breach, subject to relevant disciplinary remedies.

5.5.5 The table below outlines the roles and responsibilities of the stakeholders responsible for governance of this Policy

Responsibility	Structure	Interest, Duties and Responsibilities
Supervision	Board of Directors	The Board of Directors is responsible for Ensuring that its operations, processes, data, information, and activities are underpinned by a strong system of governance that is fully integrated into all aspects of its business. The Board remains accountable for the ongoing sustainability of the Group.
	Audit Committee	The Audit Committee is responsible for the governance of internal audit's assessment of Compliance with this Framework. It is responsible for assigning and monitoring remediation of any non-compliance or other findings by internal Audit.
Strategic / Direction	Data Governance Committee(s) (DGC)	The DGC is responsible for establishing and driving strategic direction for the Group concerning data management practices and maximizes the value derived from data assets. Itdelegates to various forums and/or persons to address or monitor operational matters including the Data Management Council.
Tactical / Operational Implementation	Data Management Council (DMC)	The DMC consists of business unit level Business Sponsors who are accountable to implement, monitor and manage the operation of data management practices.

6. Glossary of Abbreviations and Definitions

6.1 Outline

6.1.1 This section includes definitions for all terms used within this policy, including acronyms where applicable.

Term	Description
Data subjects	Any AF customer, employee, vendor and their employees or any other entity (both natural or juristic entities)
Data virtualization	Data virtualization is an approach to data management that allows an application to retrieve and manipulate data without requiring technical details about the data, such as how it is formatted at source, or where it is physically located, and can provide a single customer view (or single view of any other entity) of the overall data
Data Classification	A process of organizing data into categories that make it is easy to retrieve, sort and store for future use.
Data Steward	Officials within an organization tasked with utilizing an organization's data governance processes to ensure fitness of data elements - both the content and metadata. Stewards have a specialist role that incorporates processes, policies, guidelines, and responsibilities for administering organizations' entire data in compliance with policy and/or regulatory obligations.
DM BOK2, 2017	DAMA International is dedicated to advancing the concepts and practices of information and data management and supporting DAMA members and their organizations to address their information and data management needs. To fulfil this mission, DAMA sponsors and facilitates the development of the Data Management Body of Knowledge (the DMBoK) through its community of experts as well as developing certification and training programs. https://www.dama.org/cpages/body-of-knowledge
Document Control Register	A list, which identifies all Alexander Forbes documents and includes current revision status.
Person	means a natural person or a juristic person
Personal Information	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to ▪ information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person. ▪ information relating to the education or the medical, financial, criminal or employment history of the person. ▪ any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person. ▪ the biometric information of the person. ▪ the personal opinions, views or preferences of the person. ▪ correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and ▪ the name of the person if it appears with other personal information

Term	Description
	relating to the person or if the disclosure of the name itself would reveal information about the person
Special personal information	means personal information as referred to in section 26 of the POPIA act
Promotion of Access to Information Act (PAIA)	means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
Processing	means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including— ▪ the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use. ▪ dissemination by means of transmission, distribution or making available in any other form; or ▪ merging, linking, as well as restriction, degradation, erasure, or destruction of information
Public record	means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body;
Record	means any recorded information regardless of form or medium, including any of the following: ▪ writing on any material. ▪ information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored. ▪ label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means. ▪ book, map, plan, graph, or drawing. ▪ photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced. o in the possession or under the control of a responsible party. o whether or not it was created by a responsible party; and o regardless of when it came into existence
Structured Records	Any records that reside in a fixed field within a record or file. Structured records have well-defined structure or organisation arranged in a definite pattern.
Semi-Structured Records	Records that do not conform to the formal structure of database-based models, however, does have some predefined and predictable structure that makes it easier to analyse with the right tools and skills. Structured pdf – e.g., invoices, statements, policy schedules, xml, csv, json, NoSQL db.
Unstructured Records	Record formats appears to be random. Although structural patterns can exist, they are less predictable and harder (not impossible) to mine. E.g., physical / printed documents, excel, PowerPoints, audio-visual recordings, BlueJeans, photos, email, social media.
De-identify	De-identify in relation to personal information of a data subject, means to delete any information that: ▪ identifies the data subject. ▪ can be used or manipulated by a reasonably foreseeable method to identify the data subject; or ▪ can be linked by a reasonably foreseeable method to other information that identifies the data subject, and *"de-identified"* has a corresponding meaning;
Re-identify	in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that:

Term	Description
	▪ identifies the data subject. ▪ can be used or manipulated by a reasonably foreseeable method to identify the data subject; or ▪ can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ‘‘re-identified’’ has a corresponding meaning;
Unique identifier	means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.
Operator	means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party
Responsible party	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;
POPIA condition seven (7) Security safeguards	As summarized in POPIA sections: ▪ Section 19 Security measures on integrity and confidentiality of personal information ▪ Section 20 Information processed by operator or person acting under authority ▪ Section 21 Security measures regarding information processed by operator ▪ Section 22 Notification of security compromises

7 Approval and Administration

7.1 Approval of this Policy document

POLICY NAME	Data Governance Management
POLICY OWNER	Executive: Services
EFFECTIVE DATE	01 August 2022
LAST APPROVED	03 May 2022
APPROVAL	Data Governance Steering Committee
VERSION	2.0
LAST REVIEW DATE	03 May 2022
NEXT REVIEW DATE	12 Months from approval date
DISTRIBUTION LIST	ALL Staff

7.2 Revision History

Version	Date	Revision Author	Summary of changes
1.1	24-11-2017	Sapiens	Updated as per EY comments
1.2	28-11-2017	Sapiens	Updated as per revisions with AF
1.3	18-01-2018	Sapiens	Updated formatting as per AF review
1.4	09-02-2018	Sapiens	Moved R&R to combined document
1.5	11-04-2018	Alexander Forbes	Issued Final Draft post EY review
1.6	19-03-2019	Alexander Forbes - IT	Updated the content
1.7	03-07-2019	Alexander Forbes - Data CoE	Updated the Content
2.0	5-01-2022	Alexander Forbes - Data CoE	Updated as part of our POPIA project and annual review