

SCM DMA (Pty) Ltd

Registration number 2009/003513/07

FSP number 40983

(the "Company")

Retention of Documents Policy

(the "Policy")

1. Policy approval and information

Policy drafter	Gigi Vorlaufer
Policy reviewer	Peter Johnson
Policy creation date (1 st version)	February 2021
Policy review date (this version)	July 2021
Approver's signature	
Approved by (this version)	Board of directors

2. Retention and confidentiality of documents, information, and electronic transactions

2.1. Purpose and scope

The purpose of this Policy is to exercise effective control over the retention and confidentiality of documents, information, and electronic transactions, as prescribed by legislation and as dictated by business practice.

Documents must be retained, in accordance with legislation, to prove the existence of facts, and to exercise the rights of the Company. Documents are also necessary for defending legal action, for establishing what was said, or done, in relation to the functions of the Company, and to mitigate the Company's reputational risks.

This Policy also helps to ensure that the Company's interests are protected and that the Company's and clients' rights to privacy and confidentiality are not breached. The Policy applies to all documents, information, and electronic transactions, generated within, and/or received by, the Company.

Queries may be referred to the compliance function, or the information officer.

2.2. Legislative framework

The reference to legislation, subordinate legislation and supervision documents includes amendments made from time to time.

- Financial Sector Regulation Act 9 of 2017 (the FSRA)
- Conduct of Financial Institutions Bill (the COFI Bill)
- Protection of Personal Information Act 4 of 2014 (the POPI Act)
- Promotion of Access to Information Act 2 of 2000 (the PAIA)
- Financial Intelligence Centre Act 38 of 2001 (the FICA)
- Income Tax Act 58 of 1962

- Tax Administration Act 28 of 2011
- Value Added Tax Act 89 of 1991
- Exchange Control Regulations, as published by the South African Reserve Bank
- Constitution of the Republic of South Africa, 1996 (the Constitution)
- Financial Advisory and Intermediary Services Act 37 of 2002 (the FAIS Act)
- Companies Act 71 of 2008
- Pension Funds Act 24 of 1956 (the PFA)
- Electronic Communications and Transactions Act 25 of 2002 (the ECTA)

2.3. Definitions

The below definitions, which are not elsewhere included in this Policy, are relevant.

- 2.3.1. **Clients** includes, but is not limited to, persons that the Company has business relationships with, persons to whom the Company provides financial products or services, shareholders, debtors, creditors, as well as the affected employees and/or departments, relating to the functions of the Company;
- 2.3.2. **Confidential information** refers to all information, or data, disclosed to, or obtained by, the Company, by any means whatsoever;
- 2.3.3. **Data** refers to electronic representations of information, in any form;
- 2.3.4. **Documents** includes books, records, security, or accounts, and any information that has been stored, or recorded, electronically, magnetically, mechanically, electromechanically, or optically, or in any other form;
- 2.3.5. **Electronic communication** refers to a communication by means of data messages;
- 2.3.6. **Electronic signature** refers to data attached to, incorporated in, or logically associated with, other data, and which is intended by the user/person to serve as a signature;
- 2.3.7. **Electronic transactions** include emails sent and received.

2.4. Access to documents

- 2.4.1. All Company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:
- where disclosure is compulsory in terms of legislation;
 - where there is a duty to the public to disclose;
 - where the interests of the Company require disclosure; and

- where disclosure is made with the express or implied consent of the client.

2.5. Disclosure to third parties

2.5.1. Employees have a duty of confidentiality to the Company and its clients.

2.5.2. The Company's clients' right to confidentiality is protected in the Constitution and in terms of the ECTA. Information may only be given to a third party if the client has consented, in writing, to that person receiving the information.

Requests for the Company's information are dealt with in terms of the PAIA, which gives effect to the constitutional right of access to information held by the State, or any person (natural and juristic), that is required for the exercise, or protection, of rights. However, private bodies, like the Company, must refuse access to records, if disclosure would constitute an action of breaching the duty of secrecy owed to a third party.

2.5.3. Requests must be made in writing, on the prescribed form, to the compliance function, or the information officer. The requesting party must state the reason for wanting the information and must pay a prescribed fee.

2.5.4. Confidential company and/or business information may not be disclosed to third parties, as this may constitute industrial espionage. The affairs of the Company must always be kept strictly confidential.

2.5.5. The Company views any contravention of this Policy very seriously, and employees who are guilty of contravening the Policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

2.6. Retaining documents

Certain legislation specifies requirements for documents that must be retained, as well as how long those documents must be retained, some of which are detailed below.

2.6.1. Companies Act

7 YEARS: Hard copies of the following documents must be retained:

- Any documents, accounts, books, writing, records, or other information, that a company is required to keep, in terms of the Act
- Notice and minutes of all shareholder meetings, including resolutions adopted and documents made available to holders of securities
- Copies of reports presented at the annual general meeting of the Company

- Copies of annual financial statements, required by the Act
- Copies of accounting records, required by the Act
- Records of directors and past directors, after the director has retired from the Company
- Written communication to holders of securities
- Minutes and resolutions of directors' meetings, audit, and risk committee meetings.

INDEFINITELY: Copies of the following documents must be retained:

- Registration certificate
- Memorandum of Incorporation and alterations and amendments thereto
- Rules of the Company (if applicable)
- Securities register and uncertified securities register
- Register of company secretary and auditors
- Register of disclosure of persons who hold a beneficial interest equal to, or in excess of, 5% of the securities of that class issued (for regulated companies, i.e. companies to which chapter 5, part B, C and Takeover Regulations apply).

2.6.2. Financial Advisory and Intermediary Services Act

AT LEAST 5 YEARS: An authorised financial services provider (FSP) must retain the following records for, except to the extent exempted by the Authority:

- known premature cancellations of transactions, or financial products, by clients of the provider
- complaints received, together with an indication of whether, or not, the complaint has been resolved
- continued compliance with the requirements relating to the application for authorisation section of the Act
- cases of non-compliance with the Act, and the reasons for the non-compliance
- continued compliance by representatives, with the requirements applicable to representatives, including:
 - Before rendering a financial service, providing clients with confirmation, certified by the FSP, that a service contract, or other mandate, to represent the FSP, exists, and that the FSP accepts responsibility for those activities of the representative performed within the scope of, or in the course of implementing, the contract or mandate
 - Fit and proper requirements

- Aspects of the General Code of Conduct applicable to representatives
- Rendering financial services, or contracting, in the name of the FSP that they are representing.
- FSPs must have appropriate procedures and systems in place to record verbal and written communication relating to a financial service rendered to a client.
- FSPs must have appropriate procedures and systems in place to store and retrieve the records of verbal and written communication relating to a financial service rendered to a client, as well as any other material documents relating to the client, or the financial service rendered to the client.
- FSPs must have appropriate procedures and systems in place to keep the client records and documents safe from destruction.
- All client records and documents must be kept for 5 years after termination of the product concerned and the financial service rendered.
- records may be kept by third-parties but must be available for inspection within 7 days of the Authority's request.
- Records may be kept in an appropriate electronic, or recorded, format, which must be accessible and readily reducible to written, or printed form.
- An FSP may not disclose any confidential information acquired, or obtained, from a client, or product supplier, regarding the client, or product supplier, unless the prior written consent has been obtained from the client, or product supplier, unless the disclosure of the information is required in the public interest, or under any law.

2.6.3. Financial Intelligence Centre Act

AT LEAST 5 YEARS: As part of the customer due diligence process, employees must ensure that all records relating to the customer due diligence information obtained about clients, or prospective clients, are kept. These records must **be kept for at least 5 years from the date that the business relationship is terminated, or from the date of the conclusion of the single transaction, respectively.**

- The records must include:
 - copies of, or references to, information provided to, or obtained by, the Company, to verify a person's identity; and
 - in addition, for business relationships, information about:
 - 2.6.3.1. the nature of the business relationship;
 - 2.6.3.2. the intended purpose of the business relationship; and
 - 2.6.3.3. the source of the funds that the prospective client expects to use

for transacting during the business relationship.

- The Company will keep record of every transaction, whether the transaction is a single transaction, or concluded during a business relationship, which transactions are reasonably necessary to enable that transaction to be readily reconstructed.
- The records must include:
 - amount involved and the currency in which it was denominated
 - date on which the transaction was concluded
 - parties to the transaction
 - nature of the transaction
 - business correspondence
 - if the Company provides account facilities to its clients, the identifying particulars of all accounts, and the account files at the Company that are related to the transaction.
- **AT LEAST 5 YEARS:** These records must **be kept for at least five 5 years from the date that the transaction was concluded.**
- The Company must ensure that electronically kept records are backed-up frequently and can be reproduced in a legible format.
- The person responsible for reporting to the Financial Intelligence Centre (Centre) (or his/her alternatives, if the responsible person is not available) will keep records of transactions, or activities, that give rise to a Suspicious Activity Report or Suspicious Transaction Report, for at least 5 years from the date that the report was submitted to the Centre.
- If the Company has appointed a third party to keep records on its behalf, the Company will **immediately provide the Centre and the relevant departments of the Authority with the following details of the third party:**
 - full name, if the third party is a natural person
 - registered name, if the third party is a close corporation or company
 - name under which the third-party conducts business
 - full name and contact particulars of the individual who exercises control over access to the records
 - address where the records are kept
 - address from where the third-party exercises control over the records
 - full name and contact particulars of the individual who liaises with the third party, on behalf of the Company, regarding the retention of the records.
- The Company will ensure that it has easy access to the customer due

diligence and transaction records, and that they are readily available to the Centre and the relevant departments of the Authority.

- The Company notes that if it **fails to provide the Centre and the relevant departments of the Authority with the details of the third-party**, it is non-compliant and is subject to an **administrative sanction**.

2.6.4. Tax administration Act

- **5 YEARS:**
 - Taxpayers that have submitted a return (from date of submission)
 - Taxpayers who were not required to submit a return, but received income, had capital gains/losses or engaged in any other activity that is subject to tax, or would be subject to tax but for the application of a threshold or exemption (from the end of the relevant tax period)
- **INDEFINITE:** Taxpayers who were meant to submit a return but have not for that period (until the return is submitted, then 5 years)
- **UNTIL AUDIT IS CONCLUDED, OR ASSESSMENT, OR DECISION, BECOMES FINAL (IN ADDITION TO 5-YEAR RULE)**

○ A person who has been notified of, or is aware, that the records are subject to an audit or investigation. The extended retention period will apply irrespective of whether the assessments have prescribed.
- A person who has lodged an objection or appeal against an assessment or decision.
- **UNTIL BASE COST CALCULATION MUST BE PROVED TO SARS FOR CAPITAL GAIN/LOSS**

○ A taxpayer bears the onus of proving a valuation, an exemption, and a deduction, where any of these items form part of a calculation, for purposes of calculating the base cost for capital gains tax purposes, it is recommended that a taxpayer retain records for a longer period, because it will enable the taxpayer to discharge this onus.

2.6.5. Income Tax Act (additional to the Tax administration Act retention requirements)

- **5 YEARS FROM DATE OF SUBMITTING EMP201 & EMP501:**
 - For each employee, the employer must keep a record of:
 - 2.6.5.1. amount of remuneration paid, or due, by him, to the employee;
 - 2.6.5.2. amount of employees' tax deducted, or withheld, from the remuneration paid, or due;
 - 2.6.5.3. income tax reference number of that employee;

2.6.5.4. any further prescribed information

- **5 YEARS FROM DATE OF SUBMISSION, OR FROM END OF TAX YEAR (as applicable):**
 - Registered micro businesses must only retain records of:
 - 2.6.5.1. amounts received during a year of assessment;
 - 2.6.5.2. dividends declared during a year of assessment;
 - 2.6.5.3. each asset as at the end of a year of assessment with a cost price of more than R10 000;
 - 2.6.5.4. each liability as at the end of a year of assessment that exceeded R10 000.

2.6.6. Value Added Tax Act (additional to the Tax administration Act retention requirements)

- **5 YEARS FROM SUBMISSION DATE:**
 - Where the zero rate is applied by any vendor, documentary proof must be obtained, and retained, to substantiate the entitlement to the zero rate
 - Where a vendor's basis of accounting is changed, the vendor must prepare lists of debtors, and creditors, showing the amounts owing by the debtors, and owing to the creditors, at the end of the tax period immediately preceding the changeover period
 - record of all goods, and services, supplied by, and to, the vendor, showing the goods, and services, the rate of tax applicable to the supply, and the suppliers, or their agents, in sufficient detail, to enable the goods, and services, the rate of tax, the suppliers, or the agents, to be readily identified by the Commissioner, and all invoices, tax invoices, credit notes, debit notes, bank statements, deposit slips, stock lists, and paid cheques
 - record of all importation of goods
 - documentary proof, where tax fractions apply, and alternative documentary proof (where applicable)
 - charts, and codes, of account, the accounting instruction manuals, and the system, and programme, documents, which describes the accounting system used for each tax period, in the supply of goods, and services;
 - any list required to be prepared (i.e. vendor's basis of accounting is changed)
 - any documentary proof (i.e. zero rate is applied)

2.7. Destruction of documents

2.7.1. Documents may be destroyed after the termination of the retention period specified in the relevant legislation.

2.7.2. Each department is responsible for attending to the destruction of its documents, which must be

done regularly. Files must be checked, to ensure that the documents may be destroyed, and to ascertain whether there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company, pending return.

2.7.3. After performing this process, the head of the relevant department shall, in writing, authorise the removal and destruction of the documents in the authorisation document.

2.7.4. The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This helps to ensure confidentiality of information.

2.7.5. Documents may also be stored off-site, in storage facilities, approved by the Company, as long as the relevant authorities are informed thereof.

3. Consequences of non-compliance with the policy

3.1. All employees are obliged to comply with the Policy, and it is a condition of employment. Non-compliance is a breach of their employment contract, and is an action of misconduct, so employees may be subject to disciplinary action, which may lead to dismissal. Non-compliance by an employee will be dealt with according to the Company's disciplinary policy. For assessing, and addressing, the non-compliance, reports made by the compliance officers, internal audit, external audit, and the Authorities, will be considered, for appropriate action to be taken.

4. Policy review

4.1. The policy will be reviewed annually, updated, if necessary, and the latest version will be adopted and approved by the board where material changes have been made that necessitate board approval.