TYGERBERG GESINSKERK

POLICY ON THE CONFIDENTIALITY AND RETENTION OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

Document Ref.	POPI-3
Version:	1.0
Dated:	29 June 2021

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date
J L Delport	Head of Organisation		29 June 2021
R D le Roux	Information Officer		29 June 2021

Table of Contents:

1. PURPOSE

The purpose of this Policy is to:

1.1 To provide guidelines for the Organisation to exercise effective control over the retention of Personal Information, Records and Electronic Transactions:-

1.1.1 as prescribed by legislation; and

1.1.2 as dictated by business practice.

1.2 To ensure that the Organisation's interests are protected and that the Organisation's and its Clients', Congregants' and Visitors' rights to privacy and confidentiality are not breached.

1.3 To give effect to Section 10 and 14 of the Protection of Information Act, 4 of 2013 ("POPI") and Article 5 of the EU General Data Protection Regulation, regarding the "Retention and Restriction of Records" and "Minimality" as peremptory conditions for the lawful processing of personal information, whether as a responsible party or an operator.

1.4 To regulate the retention of certain categories of information for specific periods as mandated by statute or other applicable regulations.

1.5 To ensure that records of personal information are not retained any longer than is necessary for achieving the purpose for which the information was collected or processed, unless it is justified in terms of POPI.

1.6 To ensure that the Organisation's guidelines on retention are consistently applied throughout the organisation.

2. APPLICABILITY

This Policy applies to every Employee, shareholder and Contractor of the Organisation.

3. SCOPE & DEFINITIONS

3.1. The scope of this policy covers all Personal Information under the Organisation's control or in its possession regardless of its form or location.

3.2. Definitions:

3.2.1. **"Clients"** includes, but are not limited to, current, past and future clients that received or receives or will receive services from the Organisation or who leases the Organisation's premises.

3.2.2. **"Confidential Information"** refers to all information or data disclosed to or obtained by the Organisation by any means whatsoever and shall include, but not be limited to:

3.2.2.1. financial information and Records;

3.2.2.2. Personal Information; and

3.2.2.3. all other information including information relating to the structure, operations, processes, intentions, product

information, know-how, trade secrets, market opportunities, Clients, Congregants, Visitors and business affairs.

3.2.3. "**Congregant**" means an individual who voluntarily associates with the Organisation and has formally joined as a member.

3.2.4. **"Data Subject"** has the meaning assigned to it in terms of POPI.

3.2.5. **"Documents"** means to include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

3.2.6. **"ECTA**" means the Electronic Communications and Transactions Act, 25 of 2002.

3.2.7. **"Electronic communication"** refers to a communication by means of data messages.

3.2.8. **"Electronic signature"** refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

3.2.9. **"Electronic transactions"** include e-mails sent and received.

3.2.10. **"Employees"** means any person who is employed by the Organisation or a person who voluntarily provides a service to the Organisation.

3.2.11. **"Information Officer"** means the person appointed as such by the Organisation, from time to time.

3.2.12. "**Organisation"** means Tygerberg Gesinskerk, with registration number 930 029 157, a nonprofit organisation duly registered and incorporated in accordance with the Nonprofit Organisation Act 71 of 1997 and having its registered address at Palm Grove Centre, corner Chruch Street and Main Road, Durbanville, 7550;

3.2.13. **"PAIA"** means Promotion of Access to Information Act, 2 of 2000.

3.2.14. **"Personal Information"** has the meaning assigned to it in terms of POPI.

3.2.15. **"Policy"** means this Policy on the Confidentiality and Retention of Documents, Information and Electronic Transactions.

3.2.16. **"POPI"** means the Protection of Personal Information Act, 4 of 2014.

3.2.17. **"Processing**" has the meaning assigned to it in terms of POPI.

3.2.18. **"Record"** has the meaning assigned to it in terms of POPI.

3.2.19. **"Visitor"** means an individual other than a Congregant who visits the Organisation for purposes of utilising its services and who may or may not ostensibly associate with the Organisation.

4. POLICY PRINCIPLES

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

4.1.1. Documents and records must be managed properly from creation to disposal.

4.1.2. The Organisation follows sound procedures and practices for the creation, receiving, maintenance, retention and disposal of all records and data, including electronic records.

4.1.3. The records management procedures will comply with legal requirements, including those for provision of evidence in court, where applicable.

4.1.4. The Organisation will follow sound procedures for the security, privacy and confidentiality of its data, records, as well as Personal Information at its disposal.

4.1.5. The Organisation will have performance measures in place for all records management functions and conduct regular compliance reviews with these performance measures.

4.1.6. Development of records management and retention procedures and processes by the relevant Executive Manager, and implementation thereof by Organisation management and staff.

4.1.7. Availability of lockable storage and shredding facilities for use by all Employees.

4.1.8. Identification, assessment and management of records, data and information security risks.

4.1.9. Monitoring of compliance with policy and reporting of areas of concern and / or non – compliance.

4.1.10. Training of staff to ensure awareness on the policy and its attendant procedures and processes.

4.1.11. Implementing safe disposal methods for data and documents containing Organisation, Client, Congregant, Visitor and supplier sensitive and Personal Information.

4.1.12. Valuable documents and records must be secured at all times.

4.1.13. Documents and records must be accessible to authorised Employees for business purposes.

4.1.14. 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.

4.1.15. Employees being alert and actively participating in proper document and information management and security.

4.1.16. Procuring backups of information to prevent unauthorized loss.

5. CONFIDENTIALITY AND NON-DISCLOSURE OF RECORDS

Employees may not disclose the nature and contents of any Record to any person unless such disclosure is permitted in terms of the Employee's job description, contract of employment or upon written authorization from the Organisation.

6. INTEGRITY

6.1. All Records will be identified, classified, retained, stored and protected in such a manner that their integrity is not compromised.

6.2. Stringent guidelines and procedures must ensure that Records are admissible evidence in courts or disciplinary proceedings notwithstanding the fact that such records were created, distributed or stored in electronic format.

6.3. Scanning of Records from paper into an electronic format must be conducted in such a way that digital images can be proven to be an authentic copy of the original.

7. RECORDS MANAGEMENT REALISATION

The Organisation will define, plan and implement the processes that are required to realise the required quality of records management as well as the sequence and interaction of these processes. The Organisation will ensure that these processes are operated under controlled conditions and produce outputs, which meet legal requirements. This policy requires that the implementation thereof is assigned to the Information Officer.

8. AUDIT

8.1. Records management audits will be undertaken by the Information Officer on a regular basis.

8.2. The following audit types, but not limited to these, will be conducted:

8.2.1. Access and Security Audit;

8.2.2. Storage Areas Audit;

8.2.3. Physical and Electronic Filing Audit; and

8.2.4. Disposal Audit.

9. ACCESS TO DOCUMENTS

9.1. All Organisation and Client, Congregant and Visitor information must be dealt with in the strictest confidence and may only be disclosed, in the following circumstances:

9.1.1. where disclosure is compulsory under law;

9.1.2. where there is a duty to the public to disclose;

9.1.3. where the interests of the Organisation require disclosure; and

9.1.4. where disclosure is made with the express or implied consent of the Client, Congregant and Visitor.

9.2. Disclosure to 3rd parties:

9.2.1. All employees have a duty of confidentiality in relation to the Organisation and its Clients, Congregants and Visitors.

9.2.2. Information on Clients, Congregants and Visitors: Our Clients', Congregants' and Visitors' right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the Client, Congregant or Visitor has consented in writing to that person receiving the information.

9.3. Requests for Organisation information:

9.3.1. These are dealt with in terms of 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. The Organisation, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party. In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

9.3.2. The Organisation's manual in terms of PAIA/POPI, which contains the prescribed forms and details of prescribed fees, is available for inspection at the Organisation's address as stated in clause 2 above.

9.3.2.1. Confidential Organisation and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Organisation must be kept strictly confidential at all times.

9.3.2.2. The Organisation 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.

10. REQUIREMENTS IN TERMS OF POPI

10.1. No records of Personal Information in the possession or under the control of the Organisation will be retained after the purpose for which such information was collected has been achieved, unless:

10.1.1. retention is required by law;

10.1.2. the Organisation requires it for lawful purposes related to its business;

10.1.3. retention is required by contract between the Organisation and the Data Subject;

10.1.4. the Data Subject or a competent person on behalf of a minor Data Subject has consented to the retention.

10.2. Where the Organisation has used a Record of Personal Information to make a decision about a Data Subject, it must:

10.2.1. Retain the record for such period as prescribed by law;

10.2.2. If there is no prescribed period, retain the record for a period that will afford the Data Subject a reasonable opportunity to request access to the record.

11. STORAGE OF DOCUMENTS

11.1. HARD COPIES

The retention of hard copies of different categories of Records and the legislative retention period are as set out in Annexure "A", as attached hereto.

11.2. ELECTRONIC STORAGE

11.2.1. The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

11.2.1.1. Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

11.2.2. Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

12. NO RETENTION PERIOD

If no retention period is specified for a Record containing Personal Information, the Record, or a part thereof, as may be applicable, will be destroyed or de-identified, in the Organisation's discretion, as soon as its retention is no longer justified in terms of POPI, i.e. if the purpose for which the Personal Information was initially Processed, has been achieved.

13. DESTRUCTION OF DOCUMENTS

13.1. Documents may be destroyed:

13.1.1. after the termination of the retention period specified in this Policy; and

13.1.2. if, for any reason, the Organisation is no longer authorised to retain the Record in terms of POPI.

13.2. Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if 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 Organisation pending such return.

13.3. After completion of the process in 13.2 above, the Information Officer shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by the Organisation.

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

13.5. Documents may also be stored off-site, in storage facilities approved by the Organisation.

13.6. In appropriate circumstances the Organisation may authorise de-identification instead of destruction, which will be carried out with the assistance of IT professionals.

14. DATA DUPLICATION

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the Organization's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

15. ENFORCEMENT

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of Organization property (physical or intellectual) are suspected, the Organization may report such activities to the applicable authorities.

ANNEXURE A: RETENTION OF RECORDS IN TERMS OF LEGISLATION

Act	Record/Document	Retention Period
1. Companies Act, No 71 of 2008	• Any documents, accounts, books, writing, records or other information that a Organisation is required to keep in terms of the Act; • Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; • Copies of reports presented at the annual general meeting of the Organisation; • Copies of annual financial statements required by the Act; • Copies of accounting records as required by the Act; • Record of directors and past directors, after the director has retired from the Organisation; • Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee and directors' committees.	7 years
	• Registration certificate ; • Memorandum of Incorporation and alterations and amendments; • Rules; • Securities register and uncertified securities register;	Indefinitely
2. Consumer Protection Act, No 68 of 2008	• Full names, physical address, postal address and contact details; • ID number and registration number; • Contact details of public officer in case of a juristic person; • Service rendered; • Intermediary fee; • Cost to be recovered from the consumer; • Frequency of accounting to the consumer; • Amounts, sums, values, charges, fees, remuneration specified in monetary terms; • Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided; • Record of advice furnished to the consumer reflecting the basis on which the advice was given; • Written instruction sent by the intermediary to the consumer ; • Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions; • Documents Section 45 and Regulation 31 for Auctions.	3 years
3. National Credit Act, No 34 of 2005	• Records of registered activities such as an application for credit declined; • Reason for the decline of the application for credit; • Pre-agreement statements and quotes; • Documentation in support of steps taken in terms of section 81(2) of the Act; • Record of payments made;	3 years

	• Documentation in support of steps taken after default by consumer. • Record of income, expenses and cash flow; • Credit transaction flows; • Management accounts and financial statements. • All documents relating to disputes, inclusive of but not limited to, documents from the consumer; • Documents from the entity responsible for disputed information; • Documents pertaining to the investigation of the dispute; • Correspondence addressed to and received from sources of information as set out in section 70(2) of the Act and Regulation 18(7) pertaining to the issues of the disputed information. • Application for debt review; • Copies of all documents submitted by the consumer; • Copy of rejection letter; • Debt restructuring proposal; • Copy of any order made by the tribunal and/or the court and a copy of the clearance certificate. • Application for credit; • Credit agreement entered into with the consumer.	
	• Sequestrations • Administration orders.	Earlier of: 10 years/granting of rehabilitation order
	• Rehabilitation orders • Payment profile.	5 years
	• Civil Court Judgments	Earlier of: 5 years/rescission of judgment
	• Enquiries	2 years
	• Details and results of disputes lodged by the consumers	1.5 years
	• Adverse information	1 year
	• Liquidation	Unlimited
	• Debt restructuring	Upon issuing of a clearance certificate
4. Financial Intelligence Centre Act, No 38 of 2001:	• Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client; • If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the clients authority to act on behalf of that other person; • If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client;	5 years

	• The manner in which the identity of the persons referred to above was established; • The nature of that business relationship or transaction; • In the case of a transaction, the amount involved and the parties to that transaction; • All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; • The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; • Any document or copy of a document obtained by the accountable institution. These documents may also be kept in electronic format.	
5. Compensation for Occupational Injuries and Diseases Act, No 130 of 1993:	• Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
	• Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; • Records of incidents reported at work.	3 years:
	• Records of assessment and air monitoring, and the asbestos inventory; • Medical surveillance records; • Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): • Records of risk assessments and air monitoring; • Medical surveillance records. • Lead Regulations, 2001, Regulation 10: • Records of assessments and air monitoring; • Medical surveillance records. • Noise - induced Hearing Loss Regulations, 2003, Regulation 11: • All records of assessment and noise monitoring; • All medical surveillance records, including the baseline audiogram of every employee. • Hazardous Chemical Substance Regulations, 1995, Regulation 9 requires a retention period of 30 years for the documents mentioned below: • Records of assessments and air monitoring; • Medical surveillance records.	40 years
6. Basic Conditions of Employment Act, No 75 of 1997:	• Written particulars of an employee after termination of employment; • Employee's name and occupation; • Time worked by each employee; • Remuneration paid to each employee; • Date of birth of any employee under the age of 18 years.	3 years
7. Employment Equity Act, No 55 of 1998:	• Records in respect of the Organisation's workforce, employment equity plan and other records relevant to compliance with the Act;	3 years

		• Section 21 and Regulations 4(10) and (11) require a retention period of 3 years for the report which is sent to the Director General as indicated in the Act.	
8.	**Labour Relations Act, No 66 of 1995:**	• The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings; • Registered Trade Unions and registered employer's organisations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings; • Registered Trade Unions and employer's organisations must retain the ballot papers; • Records to be retained by the employer are the collective agreements and arbitration awards.	3 years
		• Registered Trade Unions and registered employer's organisations must retain a list of its members; • An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; • Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions; • The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.	Indefinite
9.	**Unemployment Insurance Act, No 63 of 2002:**	• Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.	5 years
5	**Tax Administration Act, No 28 of 2011:**	• Records of documents needed to: ○ Enable a person to observe the requirements of the Act; ○ Are specifically required under a Tax Act by the Commissioner by the public notice; ○ Will enable SARS to be satisfied that the person has observed these requirements.	5 years
6	**Income Tax Act, No 58 of 1962:**	• Amount of remuneration paid or due by him to the employee; • The amount of employees tax deducted or withheld from the remuneration paid or due; • The income tax reference number of that employee; • Any further prescribed information; • Employer Reconciliation return. • Amounts received by that registered micro business during a year of assessment; • Dividends declared by that registered micro business during a year of assessment; • Each asset as at the end of a year of assessment with cost price of more than R 10 000; • Each liability as at the end of a year of assessment that exceeded R 10 000.	5 years from submission
7	**Value Added Tax Act, No 89 of 1991**	• Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors	5 years

	showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; • Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; • Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; • Documentary proof substantiating the zero rating of supplies; • Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	
8 Transfer Duty Act, No 40 of 1949	• Record of the sale including a description of the property sold, the person by whom and the person to whom the property has been sold and the price paid for the property.	5 years

Appendix: Policy on the Confidentiality and Retention of Documents, Information and Electronic Transactions – To be Signed and returned to the Information Officer of the Organisation

I, _____ (print name), the undersigned Employee / Volunteer, have received a copy of Policy on the Confidentiality and Retention of Documents, Information and Electronic Transactions on the _____ of _____ 20___.

I understand that the Organisation's Records must be kept secure and confidential; and destroyed/de-identified once the purpose thereof has been achieved.

I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further accept the contents and agree to abide by the standards set in the document for the duration of my employment / contract with the Organisation.

I understand that the Organisation's need to implement this policy and agree to adhere thereto.

_____ _____

Employee / Volunteer Signature Information Officer Signature

_____ _____

Head of Organisation Signature Date

3.(POPI-3) RECORDS RETENTION POLICY(for approval)

Final Audit Report 2021-06-29

Created:	2021-06-29
By:	Riaan le Roux (riaanle@gmail.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAW-1qzxH8ygOLsHRQumBkzI_jestGkMcr

"3.(POPI-3) RECORDS RETENTION POLICY(for approval)" History

Document created by Riaan le Roux (riaanle@gmail.com)
2021-06-29 - 12:12:08 PM GMT- IP address: 8.35.59.38

Document emailed to Johannes Lodewikus Delport (johan@gesinskerk.co.za) for signature
2021-06-29 - 12:12:35 PM GMT

Email viewed by Johannes Lodewikus Delport (johan@gesinskerk.co.za)
2021-06-29 - 4:31:30 PM GMT- IP address: 105.184.248.159

Document e-signed by Johannes Lodewikus Delport (johan@gesinskerk.co.za)
Signature Date: 2021-06-29 - 4:33:02 PM GMT - Time Source: server- IP address: 105.184.248.159

Agreement completed.
2021-06-29 - 4:33:02 PM GMT