NG KERK KEMPTON KRUIN

PROTECTION OF PERSONAL INFORMATION ACT ("POPI") POLICY

Document Ref.	POPI-5
Version:	1.0
Dated:	29 June 2021

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

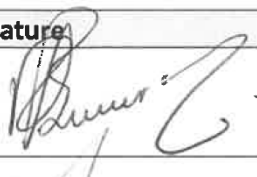
Name	Position	Signature	Date
R J Burger	Head of Organisation		29 June 2021
J Marais	Information Officer		29 June 2021

Table of Contents:

1. DEFINITIONS

In this Policy, unless the context indicates a contrary intention, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings:

1.1. "**Act**" means the Protection of Personal Information Act, Act No. 4 of 2013 (as amended);

1.2. **"Biometrics"** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

1.3. **"Client"** refers to any juristic or natural person, including a Congregant or Visitor, who deals with the Organisation and or received or receives a service from the Organisation or who utilises the Organisation's premises;

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

1.5. **"Compliance Framework"** means the Compliance Management Framework adopted by the Organisation to ensure that the necessary steps are followed to comply with POPI;

1.6. **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

1.7. "**Data Subject**" refers to the natural or juristic person to whom personal information relates, such as an individual client, congregant, visitor or an entity that supplies the organisation with products, goods or services.

1.8. "**De-Identify"** means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject;

1.9. "**Direct Marketing"** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

1.9.1. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

1.9.2. Requesting the data subject to make a donation of any kind for any reason.

1.10. "**Directors**" means the directors of the Organisation;

1.11. "**Employee/s/**" means any person, who works for the Organisation and who receives, or is entitled to receive, any remuneration, and any other person who in any manner assists in carrying on or conducting the business of the Organisation;

1.12. **"Filing System"** means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

1.13. "**Information Officer**" means the designated compliance officer appointed by the Organisation to address compliance with the Act, from time to time;

1.14. **"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. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

1.15. "**Organisation**" means NG Kerk Kempton Kruin, with P B O registration number 930 007 184, a nonprofit organisation duly registered and incorporated in accordance with the Nonprofit Organisation Act 71 of 1997 and having its registered address at 30 Fiskaal Str, Glen Marais, Kempton Park, 1619;

1.16. **"PAIA"** means the Promotion of Access to Information Act,

1.17. **"Personal Information"** shall have the meaning assigned to it in terms of POPI;

1.18. **"Personal Information Impact Assessment"**

1.19. **"Personnel"** refers to

1.19.1. any person who works for, or provides services to or on behalf of the Organisation, and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the Organisation, which includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff as well as contract workers;

1.19.2. any person who voluntarily works for, or provides services to or on behalf of the Organisation, and receives no remuneration.

1.20. "**Policy**" means this Protection of Personal Information ("POPI") Policy and any addendum thereto as may be amended by the Organisation;

1.21. **"POPI"** means the Protection of Personal Information Act, 3 of 2014;

1.22. **"Processing"** means the act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

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

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

1.22.3. merging, linking, as well as any restriction, degradation, erasure or destruction of information.

1.23. **"Re-Identify"** means in relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject;

1.24. **"Record"** Means any recorded information, regardless of form or medium, including:

1.24.1.1. Writing on any material;

1.24.1.2. 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;

1.24.1.3. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

1.24.1.4. Book, map, plan, graph or drawing;

1.24.1.5. Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

1.25. **"Regulations"** means the Regulations relating to POPI;

1.26. **"Responsible Party/Employee"** The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the Organisation is the responsible party.

1.27. **"Special Personal Information"** shall have the meaning assigned to it in terms of POPI;

1.28. **"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.

1.29. **"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,

2. INTRODUCTION

2.1. The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPI").

2.2. POPI aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the Processing of Personal Information in a context-sensitive manner.

2.3. Through the provision of quality goods and services, the Organisation is necessarily involved in the collection, use and disclosure of certain aspects of the Personal Information of Clients, Congregants, Visitors, Employees and other stakeholders.

2.4. A person's right to privacy entails having control over his, her or its Personal Information and being able to conduct his or her affairs relatively free from unwanted intrusions.

2.5. Given the importance of privacy, the Organisation is committed to effectively managing Personal Information in accordance with POPI's provisions.

2.6. This policy describes the Organisation's guidelines with regard to:-

2.6.1. Use personal information in the office;

2.6.2. Access to and disclosure of personal information sent or received by employees or contractors of the Organisation with use of the Organisation email system;

2.6.3. The processing of personal information; and

2.6.4. How to protect the Organisation from the risks of breach of security and/or unauthorized access to personal information.

3. PURPOSE

3.1. The purpose of this policy is to protect the Organisation from the compliance risks associated with the protection of personal information which includes:

3.1.1. Breaches of confidentiality. For instance, the Organisation could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.

3.1.2. Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the Organisation uses information relating to them.

3.1.3. Reputational damage. For instance, the Organisation could suffer a decline in membership following an adverse event such as a computer hacker deleting the personal information held by the Organisation.

3.2. This policy demonstrates the Organisation's commitment to protecting the privacy rights of data subjects in the following manner:

3.2.1. Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.

3.2.2. By cultivating a Organisation culture that recognises privacy as a valuable human right.

3.2.3. By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

3.2.4. By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Organisation.

3.2.5. By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer, in order to protect the interests of the organization and data subjects.

3.2.6. By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. APPLICABILITY

4.1. This policy applies to:

4.1.1. The Organisation's governing body;

4.1.2. All branches, business units and divisions of the Organisation;

4.1.3. All employees, personnel and volunteers;

4.1.4. All contractors, suppliers and other persons acting on behalf of the Organisation;

4.2. The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the Organisation's PAIA Manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).

4.3. The legal duty to comply with POPIA's provisions is activated in any situation where there is:

4.3.1. A processing of:

4.3.1.1. personal information

4.3.1.2. entered into a record

4.3.1.3. by or for a responsible person

4.3.1.4. who is domiciled in South Africa

4.4. POPIA does not apply in situations where the processing of personal information is concluded in the course of purely personal or household activities, or where the personal information has been de-identified.

5. INFORMATION OFFICER

5.1. The Organisation duly appoints **Jacobus Marais** as its Information Officer from the date of registration with the Information Regulator.

5.2. All Employees and/or Contractors may refer any queries, concerns or information of potential or actual breaches of personal information to the Information Officer.

6. DE-IDENTIFYING PERSONAL INFORMATION

6.1. The Organisation has a responsibility to ensure that information that is outdated or no longer needed, is discarded in manner that will no longer identify the Data Subject.

6.2. Archived information records are stored securely on or offsite and a certificate of destruction will be obtained for each archived file/ batch of Personal Information destroyed.

6.3. It is imperative that each and every Employee and/or Contractor takes all the necessary precautions to ensure the abovementioned protocols are adhered to. Should the Organisation receive any complaints of failure to protect the Data Subject's information, the claim must be disproved before the Information Officer. The consequence thereof is that the Employees and/or Contractors tasked with handling the specific information will be found guilty of contravening this Policy, the penalty thereof could lead to a written warning.

6.4. The Organisation's complaints procedure that should be followed in the event of a compliant is as follows:

6.4.1. The complaint must be reported to the Information Officer immediately;

6.4.2. The Information Officer must report the complaint to the Head of Organisation;

6.4.3. The Employees and/or Contractors implicated must furnish the Information Officer with written representations of the Employees and/or Contractors) statement under oath;

6.4.4. The Information Officer will liaise with the Regulator for any further developments regarding the matter.

7. RIGHTS OF DATA SUBJECTS

7.1. Where appropriate, the Organisation will ensure that its Clients, Congregants and Visitor are made aware of the rights conferred upon them as Data Subjects.

7.2. The Organisation will ensure that it gives effect to the following seven rights.

7.3. **The Right to Access Personal Information**

7.3.1. The Organisation recognises that a Data Subject has the right to establish whether the Organisation holds Personal Information related to him, her or it including the right to request access to that Personal Information.

7.3.2. An example of a "Personal Information Request Form" can be found under Annexure A.

7.4. **The Right to have Personal Information Corrected or Deleted**

7.4.1. The Data Subject has the right to request, where necessary, that his, her or its Personal Information must be corrected or deleted where the Organisation is no longer authorised to retain the Personal Information.

7.5. **The Right to Object to the Processing of Personal Information**

7.5.1. The Data Subject has the right, on reasonable grounds, to object to the processing of his, her or its Personal Information.

7.5.2. In such circumstances, the Organisation will give due consideration to the request and the requirements of POPI. The Organisation may cease to use or disclose the Data Subject's Personal Information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the Personal Information.

7.6. **The Right to Object to Direct Marketing**

7.6.1. The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

7.7. **The Right to Complain to the Information Regulator**

7.7.1. The Data Subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its Personal Information.

7.7.2. An example of a "POPI Complaint Form" can be found under Annexure B.

7.8. **The Right to be Informed**

7.8.1. The data subject has the right to be notified that his, her or its Personal Information is being collected by the Organisation.

7.8.2. The Data Subject also has the right to be notified in any situation where the Organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

8. REQUIREMENTS FOR LAWFUL PROCESSING

All employees and persons acting on behalf of the Organisation will at all times be subject to, and act in accordance with, the following guiding principles:

8.1. Accountability

8.1.1. Failing to comply with POPIA could potentially damage the Organisation's reputation or expose the Organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

8.1.2. The Organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Organisation will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

8.2. Processing Limitation

8.2.1. The Organisation will ensure that personal information under its control is processed:

8.2.1.1. in a fair, lawful and non-excessive manner, and

8.2.1.2. only with the informed consent of the data subject, and

8.2.1.3. only for a specifically defined purpose.

8.2.1. The Organisation will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

8.2.2. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the Organisation will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

8.2.3. The Organisation will under no circumstances distribute or share personal information between separate legal entities, associated Organisations or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

8.2.4. Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the Organisation's business and be provided with the reasons for doing so.

8.3. Purpose Specification

8.3.1. All of the Organisation's business units and operations must be informed by the principle of transparency.

8.3.2. The Organisation will process personal information only for specific, explicitly defined and legitimate reasons.

8.3.3. The Organisation will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

8.4. **Further Processing Limitation**

8.4.1. Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

8.4.2. Therefore, where the Organisation seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the Organisation will first obtain additional consent from the data subject.

8.5. **Information Quality**

8.5.1. The Organisation will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

8.5.2. The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the Organisation will put into ensuring its accuracy.

8.5.3. Where personal information is collected or received from third parties, the Organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

8.6. **Open Communication**

8.6.1. The Organisation will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

8.6.2. The Organisation can be contacted on the following email addresses: ontvangs@kruin-kerk.co.za and cobus@kruin-kerk.co.za to:

8.6.2.1. Enquire whether the Organisation holds related personal information, or

8.6.2.2. Request access to related personal information, or

8.6.2.3. Request the Organisation to update or correct related personal information, or

8.6.2.4. Make a complaint concerning the processing of personal information.

8.7. **Security Safeguards**

8.7.1. The Organisation will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

8.7.2. Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as religious convictions and sexual orientation, the greater the security required. The Organisation will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Organisation's IT network.

8.7.3. The Organisation will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

8.7.4. All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the Organisations responsible.

8.7.5. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

8.7.6. The Organisation's operators and third-party service providers will be required to enter into service level agreements with the Organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

8.7.7. Written Records will be kept secure:

8.7.7.1. Personal Information records should be kept in locked cabinets, or safes.

8.7.7.2. When in use Personal Information records should not be left unattended in areas where non-staff members may access them.

8.7.7.3. The Organisation shall implement and maintain a "Clean Desk Policy" where all staff shall be required to clear their desks of all personal information any kind when leaving their desks for any length of time and at the end of the day.

8.7.7.4. Personal Information which is no longer required should be disposed of by shredding.

8.7.7.5. Any loss or theft of, or unauthorised access to, personal information must be immediately reported to the Information Officer.

8.7.8. Electronic records of any kind will be kept secure:

8.7.8.1. All electronically held Personal Information must be saved in a secure database.

8.7.8.2. As far as reasonably practicable, no Personal Information of data subjects of the Organisation should be saved on individual computers, laptops or hand-held devices.

8.7.8.3. All computers, laptops and hand-held devices should be access protected with a password, fingerprint or with the password or screen finger scan being of reasonable complexity and changed frequently.

8.7.8.4. All staff of the Organisation shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day.

8.7.8.5. Electronic Personal Information which is no longer required must be deleted from the individual laptop, handheld device or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable. 9. Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

8.7.9. Passwords and Access:

8.7.9.1. Users have a responsibility to safeguard any credentials granted to them by the Organisation. In order to limit security risks, all Users must abide by the following: a. Attempts should not be made to by-pass or render ineffective security measures provided by the Organisation. b. Users may not: i. Share user IDs or usernames. ii. Divulge passwords to other users. iii. Attempt to impersonate other users. iv. Leave their computer unattended without logging out or locking v. Share passwords between users, except where they are released as part of the approved procedure. An approved procedure exists for releasing passwords where accounts are required, and staff are unavailable.

8.8. **Data Subject Participation**

8.8.1. A data subject may request the correction or deletion of his, her or its personal information held by the Organisation.

8.8.2. The Organisation will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

8.8.3. Where applicable, the Organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

9. ACCESS AND SECURITY TO INFORMATION/RECORDS

9.1. Records in all formats, shall at all times be protected against unauthorised access and tampering to protect their authenticity and reliability as evidence of the business of the Organisation.

9.2. Security classified records shall be managed only by authorised persons.

9.3. No staff member shall remove records in any format that are not available in the public domain from the premises of the Organisation without the explicit permission of the Information Officer.

9.4. No staff member shall provide information and records that are not in the public domain to the public without consulting the Information Officer. Specific guidelines regarding requests for information are contained in the POPI/PAIA Manual which is maintained by the Information Officer.

9.5. Personal information shall be managed in terms of the policy and POPI.

9.6. No staff member shall disclose personal information of any member of staff or any other data subject to any member of the public without the express prior consent of the Information Officer.

9.7. Records storage areas shall at all times be protected against unauthorised access. The following shall apply:

9.7.1. Registry and other records storage areas shall be locked when not in use.

9.7.2. Access to server rooms and storage areas for electronic records media and CCTV shall be managed with key card access or strict key control.

9.8. Paper-based records

9.8.1. No records shall be removed from paper-based files without the explicit permission of the Information Officer.

9.8.2. Records that were placed on files shall not be altered in any way.

9.8.3. No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the Information Officer.

9.8.4. Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

9.9. Electronic records

9.9.1. The Organisation shall use systems which ensure that its electronic records are:

9.9.1.1. authentic;

9.9.1.2. not altered or tampered with;

9.9.1.3. legible;

9.9.1.4. auditable; and

9.9.1.5. produced/processed in systems which utilise security measures to ensure their integrity.

10. TECHNICAL AND ORGANISATIONAL MEASURES

10.1. The Organisation will develop (or has already developed) an information security framework to:

10.1.1. Help the Organisation secure Personal Information against data breaches, leaks, or other incidents where an unauthorized party could gain access to it;

10.1.2. Identify risks to the security of the Organisation's equipment, premises, systems, networks, and other means of processing personal information; and

10.1.3. Minimize security risks, including through Personal Information Impact Assessments and monitoring.

10.2. The Organisation will assign duties to Employees within the Organisation, and where appropriate, to external persons to ensure the proper implementation of the framework.

10.3. The following technical and organizational measures will be implemented by the Organisation:

10.3.1. **Physical Controls**

10.3.1.1. **Physical access measures**: locking filing cabinets or office doors and physical access controls (such as key cards, biometrics, or other identification methods to ensure that only authorized persons have access);

10.3.1.2. **Physical monitoring:** video surveillance (CCTV systems) and security personnel;

10.3.1.3. **Hard copy records management:** shredding paper records which are no longer needed in a safe manner and enforcing clean desk policies;

10.3.1.4. **Physical privacy measures:** having private consulting and storage areas; and

10.3.1.5. **Ancillary physical measures** that physically limit or prevent access to data, be it on IT equipment, systems, or infrastructure, or in hard copy records.

10.3.2. **Technical Controls**

10.3.2.1. **Data security:** file encryption and password protection, export control and data classification;

10.3.2.2. **Equipment and systems security:** device and removable storage media encryption, user access management, mobile device management and secure disposal or re-use of equipment;

10.3.2.3. **Network and communications security:** firewalls, end-to-end encryption, digital access control, penetration testing and endpoint protection;

10.3.2.4. **Software security:** antivirus software and keeping software up to date; and

10.3.2.5. **Other measures** related to hardware or software that protects systems and resources.

10.3.3. **Operational controls**

10.3.3.1. **Operational awareness:** fostering a culture of data protection through an Employee awareness campaign;

10.3.3.2. **Training:** in-house and external (where appropriate) training to operationalize policies;

10.3.3.3. **Operational monitoring:** monitoring workstations and providing a way of reporting data breaches;

10.3.3.4. **Procedures:** employee on-boarding and exit and security procedures;

10.3.3.5. **Other measures** that involve members of the Organisation.

10.3.4. **Administrative controls**

10.3.4.1. **Administrative awareness:** director awareness and impressing management responsibility;

10.3.4.2. **Security planning:** planning around data protection, business continuity arrangements and considering acceptable standards;

10.3.4.3. **Security documentation:** drafting the necessary data protection policies and updating them regularly;

10.3.4.4. **Security assurances**: cyber insurance (if appropriate), implementing due diligence (risk assessment) procedures and implementing audit controls; and

10.3.4.5. **Other measures** that involve senior management.

10.3.5. **Continued review**

10.3.5.1. The Information Officer and relevant Employees will continually review:

10.3.5.1.1. The security of equipment, premises, systems, networks;

10.3.5.1.2. The adequacy of the information security framework;

10.3.5.1.3. Against industry security standards.

11. PERFORMING A POPI GAP ANALYSIS AND RISK ASSESSMENTS

11.1. The Organisation already takes care when processing data. However, the Organisation has to identify what areas of POPI compliance the Organisation already meets and where the Organisations deficient.

11.2. POPIA's security requirements require the Information Officer of the Organisation to take necessary measures for protecting the Organisation's information.

11.3. Risk Assessment/Gap Analysis is an opportunity to identify the Organisation's security strengths and weaknesses, and to ensure that management can cope with the information security threats the Organisation faces.

11.4. The risk assessment, is also an analysis of how Personal Information is collected, used, shared, stored, filed and maintained by the Organisation.

11.5. The Gap Analysis can reveal where the Organisation has weaknesses when it comes to protecting the Personal Information it collects, stores and uses.

11.6. Processes have to be put in place to collect data only for a specific purpose: to inform the Data Subjects of the reason for collection, and to have a process for safely deleting/destructing the data when it has served its purpose.

11.7. The gap analysis and risk assessments should normally be started early in project development or design, or before a new data processing activity, and must be considered throughout the information lifecycle from collection to destruction.

11.8. To sum it up, here are some questions to answer when the Organisations undertaking assessments:

11.8.1. Does the Organisation have the appropriate legal authority to collect personal data?

11.8.2. Have the Organisation received consent from the data subjects to use their data?

11.8.3. Is the Organisation using out-of-date or irrelevant personal data to make decisions?

11.8.4. Is the Organisation disclosing data to third parties that it is not authorised or who do not keep personal data appropriately secure?

11.8.5. Do the Organisation have processes in place to dispose of private data after use?

12. POPI AND E-MAIL USAGE

12.1. If it is needed, each Employee within the Organisations provided with a Organisation email account to assist with their work for the Organisation. This account is the primary way that Employees will communicate with Clients and other Data Subjects.

12.2. The email account of an Employee, and any information contained in it, including content, headers, directories and email system logs, remains the property of the Organisation.

12.3. Usage of the Organisation email system is exclusively for Organisation and professional purposes.

12.4. Incidental use of an e-mail account for personal purposes is allowed and is subject to the same policies and regulations as official use. However, systematic use on behalf of individuals or organisations that are not associated with the Organisation or its business is not allowed.

12.5. Employees are responsible for the integrity of their mailbox. IT Services cannot restore any emails deleted accidentally or otherwise. All email messages may be subject POPI and other legislation and laws of South Africa and any employment prescripts as amended, updated or replaced from time to time.

12.6. Although the Organisation has systems in place to protect the integrity and safety of the Organisation's electronic network, it must be noted that the Organisation cannot guarantee the confidentiality of the information stored on any network device belonging to the Organisation.

12.7. Great care should be taken when attaching documents to ensure the correct information is being released.

12.8. Any email should be regarded as a written formal letter and information.

12.9. Any defamatory or careless remarks can have very serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited.

12.10. To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received. Suspect e-mails should be deleted immediately and never forwarded to other Users.

12.11. E-mail users must be aware of the use of dangerous code by hackers and other outside parties which refers to any computer programme that causes destruction or harm and has been programmed in such a way with the malicious intent of the content of a computer or other electronic communication device. Dangerous Code is classified as file infector viruses, system or boot record viruses and macro viruses. It must be noted that viruses can either be decimated or "contracted" by the exchange of various media or by the receipt in an e-mail from a source that is unknown or spam. Effective anti-virus software will normally indicate such e-mails.

12.12. Staff and learners are not authorised to retrieve or read any e-mail messages that are not sent to them or not for their attention, except when authorised under the approved procedure.

12.13. Email messages must not be forwarded to external non-Organisation accounts such as a staff member's own personal e-mail account. Should a staff member or learner receive any offensive, unpleasant, harassing or intimidating messages via e-mail, he/she are requested to inform the Information Officer immediately.

13. COMPLIANCE MANAGEMENT FRAMEWORK

13.1. Compliance is not a "one-and-done event". It is an ongoing and active process that requires consistent management. The Organisation should have an active compliance plan in place that provides for a systematic way to review and update the Organisation's processing standards on a regular basis.

14. PROCESSING OF INFORMATION BY USING AUTOMATED AND NON-AUTOMATED MEANS

14.1. POPIA applies to the processing of any Personal Information by the Organisation that has been entered into a record by or for the Organisational the responsible party by using automated and non-automated means.

14.2. This is subject to the proviso that when the recorded Personal Information is processed by any non-automated means, the record must form part of a filing system or is intended to form part of a filing system.

15. SPECIFIC DUTIES AND RESPONSIBILITIES

15.1. Leaders /Senior Management ("Governing Body")

15.1.1. The Organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the Organisation meets its legal obligations in terms of POPI.

15.1.2. The governing body may however delegate some of its responsibilities in terms of POPI to management or other capable individuals.

15.1.3. The governing body is responsible for ensuring that:

15.1.3.1. The Organisation appoints an Information Officer.

15.1.3.2. All persons responsible for the processing of personal information on behalf of the Organisation:

15.1.3.2.1. are appropriately trained and supervised to do so,

15.1.3.2.2. understand that they are contractually obligated to protect the personal information they come into contact with, and

15.1.3.2.3. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

15.1.3.3. Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

15.1.3.4. The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the Organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

15.2. **Information Officer**

15.2.1. The Organisation's Information Officer is responsible for:

15.2.1.1. Taking steps to ensure the Organisation's reasonable compliance with the provision of POPIA.

15.2.1.2. Keeping the governing body updated about the Organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

15.2.1.3. Continually analysing privacy regulations and aligning them with the Organisation's personal information processing procedures. This will include reviewing the Organisation's information protection procedures and related policies.

15.2.1.4. Ensuring that POPI Audits are scheduled and conducted on a regular basis.

15.2.1.5. Ensuring that the Organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the Organisation. For instance, maintaining a "contact us" facility on the Organisation's website.

15.2.1.6. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the Organisation. This will include overseeing the amendment of the Organisation's employment contracts and other service level agreements.

15.2.1.7. Encouraging compliance with the conditions required for the lawful processing of personal information.

15.2.1.8. Ensuring that employees and other persons acting on behalf of the Organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the Organisation's security controls. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Organisation.

15.2.1.9. Addressing employees' POPIA related questions.

15.2.1.10. Addressing all POPIA related requests and complaints made by the Organisation's data subjects.

15.2.1.11. Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

15.2.1.12. To ensure that:-

15.2.1.12.1. A Compliance Framework is developed, implemented, monitored and maintained;

15.2.1.12.2. A Personal Information Impact Assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of Personal Information;

15.2.1.12.3. A manual is developed, monitored, maintained and made available as prescribed in terms of sections 14 and 51 of PAIA, as amended;

15.2.1.12.4. Internal measures are developed together with adequate systems to process requests for information and access thereto;

15.2.1.12.5. Internal awareness sessions are conducted regarding the provisions of POPI, Regulations, codes of conduct (if applicable) or information obtained from the Information Regulator; and

15.2.1.12.6. Upon request by any person, copies of the manual are provided to that person upon payment of a fee to be determined by the Regulator from time to time;

15.2.1.12.7. A report is submitted to the Information Regulator annually regarding the aspects set out in Regulation 6.3;

15.2.1.12.8. If requested by the Information Regulator, to furnish it with information about requests for access to the records of the Organisation.

15.3. **IT Manager**

15.3.1. The Organisation's IT Manager is responsible for:

15.3.1.1. Ensuring that the Organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.

15.3.1.2. Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.

15.3.1.3. Ensuring that servers containing personal information are sited in a secure location, away from the general office space.

15.3.1.4. Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.

15.3.1.5. Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.

15.3.1.6. Ensuring that personal information being transferred electronically is encrypted.

15.3.1.7. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.

15.3.1.8. Performing regular IT audits to ensure that the security of the Organisation's hardware and software systems are functioning properly.

15.3.1.9. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.

15.3.1.10. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the Organisation's behalf. For instance, cloud computing services.

15.4. **Marketing and Communication Manager**

15.4.1. The Organisation's Marketing & Communication Manager is responsible for:

15.4.1.1. Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Organisation's website, including those attached to communications such as emails and electronic newsletters.

15.4.1.2. Addressing any personal information protection queries from journalists or media outlets such as newspapers.

15.4.1.3. Where necessary, working with persons acting on behalf of the Organisation to ensure that any outsourced marketing initiatives comply with POPIA.

15.5. **Employees and other Persons acting on behalf of the Organisation**

15.5.1. Employees and other persons acting on behalf of the Organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

15.5.2. Employees and other persons acting on behalf of the Organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

15.5.3. Employees and other persons acting on behalf of the Organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

15.5.4. Employees and other persons acting on behalf of the Organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

15.5.5. Employees and other persons acting on behalf of the Organisation will only process personal information where:

15.5.5.1. The data subject, or a competent person where the data subject is a child, consents to the processing; or

15.5.5.2. The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or

15.5.5.3. The processing complies with an obligation imposed by law on the responsible party; or

15.5.5.4. The processing protects a legitimate interest of the data subject; or

15.5.5.5. The processing is necessary for pursuing the legitimate interests of the Organisation or of a third party to whom the information is supplied.

15.5.6. Furthermore, personal information will only be processed where the data subject:

15.5.7. Clearly understands why and for what purpose his, her or its personal information is being collected; and

15.5.8. Has granted the Organisation with explicit written consent or verbally recorded consent or reasonable

ostensible consent to process his, her or its personal information.

15.5.9. Employees and other persons acting on behalf of the Organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

15.5.10. Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

15.5.11. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Organisation will keep a voice recording of the data

15.5.12. subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

15.5.13. Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

15.5.13.1. the personal information has been made public, or

15.5.13.2. where valid consent has been given to a third party, or

15.5.13.3. the information is necessary for effective law enforcement.

15.5.14. Employees and other persons acting on behalf of the Organisation will under no circumstances:

15.5.15. Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.

15.5.16. Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the Organisation's central database or a dedicated server.

15.5.17. Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be

requested from the relevant line manager or the Information Officer.

15.5.18. Transfer personal information outside of South Africa without the express permission from the Information Officer.

15.5.19. Employees and other persons acting on behalf of the Organisation are responsible for:

15.5.19.1. Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.

15.5.19.2. Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

15.5.19.3. Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the Organisation, with the sending or sharing of personal information to or with authorised external persons.

15.5.19.4. Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

15.5.19.5. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

15.5.19.6. Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

15.5.19.7. Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

15.5.19.8. Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.

15.5.19.9. Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email.

15.5.19.10. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.

15.5.19.11. Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

15.5.19.12. Undergoing POPI Awareness training from time to time.

15.5.19.13. Where an employee, or a person acting on behalf of the Organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer.

16. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

16.1. Data subjects have the right to:

16.1.1. Request what personal information the Organisation holds about them and why.

16.1.2. Request access to their personal information.

16.1.3. Be informed how to keep their personal information up to date.

16.1.4. Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

16.1.5. Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the Organisation's PAIA Policy.

16.1.6. The Information Officer will process all requests within a reasonable time.

17. FORBIDDEN USES OF DATA SUBJECT'S PERSONAL INFORMATION

17.1. The Employee or Contractor may not use the Organisation's access to any data subject's personal information for personal gain or any such purposes as soliciting or proselytizing for commercial ventures or personal causes or outside organizations or other similar, non-job-related solicitations. If the Organisation discovers that any Employee or Contractor misusing the information available in the Organisation's systems, that particular Employee and/or Contractor will be subject to disciplinary action, which may include dismissal.

17.2. Should and Employee or Contractor be suspected of contravening this policy, the Organisation may at its sole discretion access any device which the Employee or Contractor uses to conduct business to investigate the matter further.

17.3. **Common Acts of POPI Non-Compliance:**

17.3.1. Loss or theft of paperwork/data/misfiling/not saving data.

17.3.2. Data posted or e-mailed or sent to the incorrect recipient including on any groups on any social media application or platform.

17.3.3. Insecure webpage (including hacking).

17.3.4. Loss or theft of an unencrypted device.

17.3.5. No or inadequate firewalls and/or anti-virus software.

17.3.6. Insecure disposal of paperwork.

17.3.7. Failure to redact data.

17.3.8. Sensitive or confidential information uploaded to the webpage.

17.3.9. Verbal disclosure without permission or carelessly done.

17.3.10. Insecure disposal of hardware.

17.3.11. Sending confidential data by e-mail/Apps that are not supposed to be circulated.

17.3.12. Sticky notes with PII data breach such as passwords or reminders.

17.3.13. Smartphone unsecured data breach.

17.3.14. Lost keys data breach/not keeping keys safe.

17.3.15. Lost digital/electronic items data breach (laptops, USBs, external hard drives etc.)

17.3.16. Easy access to computer room/offices.

17.3.17. Leaving file cabinets, desk drawers and cupboards open or documents on desks unattended.

17.3.18. Unsecured access card.

17.3.19. Forgotten documents in the printer/copy machine.

17.3.20. Responding to phishing e-mails/clicking on unsecured links.

18. ORGANISATION'S RIGHT TO ACCESS INFORMATION

18.1. The Organisation respects the individual privacy of its Employees and/or Contractors. However, Employee and/or Contractor privacy does not extend to the Employee's and/or Contractor's work-related conduct or to the use of Organisation provided equipment or supplies.

18.2. The electronic mail system has been installed by the Organisation to facilitate business communications. Although each Employee and/or Contractor has an individual password to access this system, it belongs to the Organisation and the contents of e-mail communications are accessible at all times by the Organisation management for any business purpose. These systems may be subject to periodic unannounced inspections and should be treated like other shared filing systems. All system passwords and encryption keys must be available to the Organisation management and the designated IT personnel, and the Employee and/or Contractor may not use passwords that are unknown to their supervisor or the designated IT personnel or install encryption programs without turning over encryption keys to their supervisor your designated IT personnel. All e-mail messages are Organisation records. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the Organisation without the Employee's and/or Contractor's permission.

18.3. Therefore, the Employee and/or Contractor should not assume that messages or telephone calls are confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

19. BREACH OF SECURITY/ UNAUTHORISED ACCESS TO INFORMATION

19.1. Should the Organisation experience any security breach, it is required, by law, to notify the Regulator; and the data subject(s) whose information have been affected by the breach, unless the identity of such data subject(s) cannot be established.

19.2. Therefore, the Employee and/or Contractor should report any known or suspected breach of information to the appointed Information Officer.

19.3. Failure to report the aforementioned breach will subject the Employee and/or Contractor in transgression to disciplinary action, which may include dismissal.

19.4. The Organisation has established a complaints process to deal with allegations of leaked information. This will be addressed by the Compliance Officer.

20. CORPORATE POLICY GUIDELINE

20.1. **Acceptable Uses of Personal Information**

20.1.1. The Organisation provides access to its server and e-mail access is intended to be for business reasons only. The Organisation encourages the use of the server and e-mail because they make communication more efficient and effective. However, the server and e-mail are Organisation property, and their purpose is to facilitate Organisation business. Every Employee and/or Contractor has a responsibility to maintain and enhance the Organisation's public image and to use Organisation-mail and access to the server in a productive manner. To ensure that all Employees and/or Contractors are responsible, the following guidelines have been established for using e-mail and the server. Any improper use of the server or e-mail is not acceptable and will not be permitted.

20.1.2. The Employee and/or Contractor acknowledges that:-

20.1.2.1. The Organisation may be held vicariously liable for the acts of its Employees and/or Contractors, even where the Organisation is not at fault, for any damages caused by the Employee's and/or Contractor's conduct;

20.1.2.2. Employees and/or Contractors may not make representations to third parties or the public beyond the scope of their normal responsibilities or actual authority;

20.1.2.3. Methods other than email must be used to communicate special personal information.

20.2. **Unacceptable Uses of Personal Information**

20.2.1. The Organisation acknowledges that Employees and/or Contractors need reasonable access to data subjects' personal information in order to fulfil their tasks.

20.2.2. The Employees and/or Contractors may not process the Employee's and/or Contractors' personal without obtaining the requisite consent, following the protocols discussed in this policy and in the Act.

20.3. **Queries and Clarification of Policy**

20.3.1. Where an employee is uncertain as to the content of this policy or requests further clarification of issues which are addressed in this policy they are required to contact the Compliance Officer for clarification.

21. MONITORING AND IMPLEMENTATION OF THE POLICY

21.1. The Governing Body (Leaders and Senior Management) as well as the Information Officer and all operators, as defined by POPIA, are responsible for administering and overseeing the implementation of this policy manual and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes.

21.2. Periodic reviews and audits will be conducted by the Information Officer where appropriate, to demonstrate compliance with POPIA, any policies and guidelines.

22. POPI COMPLAINTS PROCEDURE

Complaints may be filled via email to cobus@kruin-kerk.co.za

23. DISCIPLINARY ACTION

23.1. Where a POPI complaint or a POPI infringement investigation has been finalised, the Organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

23.2. In the case of ignorance or minor negligence, the Organisation will undertake to provide further awareness training to the employee.

23.3. Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the Organisation may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

23.4. Examples of immediate actions that may be taken subsequent to an investigation include:

23.4.1. A recommendation to commence with disciplinary action.

23.4.2. A referral to appropriate law enforcement agencies for criminal investigation.

23.4.3. Recovery of funds and assets in order to limit any prejudice or damages caused.

kruin.
— Huise wat Jesus volg —

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please download, complete and email to cobus@kruin-kerk.co.za

Please submit the completed form to the information officer:	
Name	**Jacobus Marais**
Contact Number	**076 673 9183**
Email address	cobus@kruin-kerk.co.za

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject	
Name & Surname	
Identity no	
Postal address	
Contact no	
Email address	
B. Request	
I request the Organisation to:	
(a) Inform me whether it holds any of my personal information	
(b) Provide me with a record or description of my personal information	
(c) Correct or update my personal information	
(d) Destroy or delete a record of my personal information	
C. Instructions	
D. Signature	
Signature **Date:**	

We need the Personal Information requested in this form to:

- **Locate the requested information/documentation;**
- **Give effect to your request;**
- **Send you information/documentation;**
- **Contact you regarding your request;**
- **Record particulars of the Request in a register; and**
- **Other purposes directly related to the above.**

If the Personal Information described above is being processed by a third party on our behalf, you consent that we may disclose the information herein to such third party in order to comply with your request.

ANNEXURE B: POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your Personal Information and are bound by the Protection of Personal Information Act.

Please download, complete and email to cobus@kruin-kerk.co.za

Please submit the completed form to the information officer:	
Name	Cobus Marais
Contact Number	076 673 9183
Email address	cobus@kruin-kerk.co.za

Where we are unable to resolve your complaint to your satisfaction, you have the right to complain to the Information Regulator.

Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria

Email: inforreg@justice.gov.za Website: http://www.justice.gov.za/inforeg/index.html

A. Particulars of Complainant	
Name & Surname	
Identity no	
Postal address	
Contact no	
Email address	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature	**Date:**

5.(POPI-5) POPI POLICY (for approval)

Final Audit Report 2021-06-30

Created:	2021-06-29
By:	Jacobus Marais (cobus@kruin-kerk.co.za)
Status:	Signed
Transaction ID:	

"5.(POPI-5) POPI POLICY (for approval)" History

Document created by Jacobus Marais (cobus@kruin-kerk.co.za)
2021-06-29

Document emailed to Roelof Jacobus Burger (roelf@skybegsol.co.za) for signature
2021-06-29

Email viewed by Roelof Jacobus Burger (roelf@skybegsol.co.za)
2021-06-30

Document signed by Roelof Jacobus Burger (roelf@skybegsol.co.za)
Date: 2021-06-30

Agreement completed.
2021-06-30