kruin.
—Huise wat Jesus volg —

NG KERK KEMPTON KRUIN

PERSONAL INFORMATION BREACH MANAGEMENT POLICY

Document Ref.	POPI-4
Version:	1.0
Dated:	29 June 2021

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

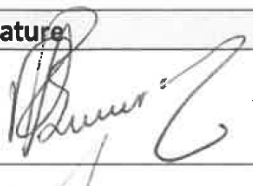
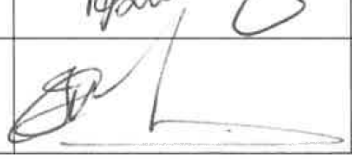
Name	Position	Signature	Date
R J Burger	Head of Organisation		29 June 2021
J Marais	Information Officer		29 June 2021

Table of Contents:

1. DEFINITIONS

1.1. **"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;

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

1.3. **"Data Subject"** has the meaning assigned to it in section 1 of POPI and includes, client, congregant and visitors;

1.4. **"Information Breach"** means any incident, event or action that has the potential to compromise the availability of Personal Information, the integrity of information, confidentiality or our Organisation's information systems. This includes incidents or events that happen by accident or deliberately. Both confirmed and suspected incidents may qualify as an Information Breach. For the purposes of this information breach policy, an incident may include (but is not limited to) any of the following:

1.4.1. Unauthorised use or accessing of information;

1.4.2. Unauthorised modification of information;

1.4.3. Loss of personal or sensitive information;

1.4.4. Theft of personal or sensitive information;

1.4.5. Loss or theft of equipment on which information has been stored;

1.4.6. Individual error;

1.4.7. Any attempts to gain access to information or our Organisation IT systems (both successful or failed);

1.4.8. Defacement of web property;

1.4.9. Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it;

1.4.10. Physical incidents, like a fire, which could compromise IT systems.

1.5. **"Organisation" / "We" / "Us"** means NG Kerk Kempton Kruin, with PBO 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;

1.6. **"Personal Information"** has the meaning assigned to it in POPI;

1.7. **"POPI"** means the Protection of Personal Information Act, 4 of 2013.

1.8. **"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. POLICY STATEMENT

2.1. NG Kerk Kempton Kruin ("the Organisation") is committed to its obligations under POPI and maintain a robust and structured program for compliance adherence and monitoring. The Organisation carries out frequent risk assessments and gap analysis reports to ensure that its compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, the Organisation recognises that breaches can occur, so this policy states its intent and objectives for dealing with such incidents.

2.2. Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect Data Subjects and their Personal Information from any risks associated with processing information. The protection and security of the Personal Information that We process is of paramount importance to us and we have developed information specific controls and protocols for any breaches relating to POPI and information protection laws.

3. PURPOSE

3.1. The purpose of this policy is to provide the Organisation's intent, objectives and procedures regarding Information Breaches involving Personal Information. As we have obligations under POPI, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees, ensuring that they are aware of what the protocols and reporting lines there are for Personal Information Breaches. This policy details our processes for reporting, communicating and investigating Information Breaches**.**

4. SCOPE

4.1. This policy applies to all persons within the Organisation (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Organisation). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5. INFORMATION SECURITY & BREACH REQUIREMENTS

5.1. We have a legal, regulatory and business obligation to ensure that Personal Information is protected whilst being processed by the Organisation. Our technical and organisational measures are detailed in our POPI Privacy Policy.

5.2. We carry out information audits to ensure that all Personal Information processed by Us is accounted for and recorded, alongside risk assessments that assess the scope and impact of any potential information breach; both on the processing and on a Data Subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including (but not limited to):

5.2.1. Restricted access;

5.2.2. Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3. Up-to-date and secure backups and the ability to restore the availability and access to Personal Information in a timely manner in the event of an Information Breach;

5.2.4. Audit procedures and stress testing on a regular basis to test, assess, review and evaluate the effectiveness of all measures;

5.2.5. Frequent training programs for all staff in POPI, its principles and applying those regulations to each role, duty and the Organisation as a whole;

5.2.6. Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the information protection regulations and the measures we have in place to protect Personal Information;

5.2.7. Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Information Officer.

6. OBJECTIVES

6.1. To adhere to POPI and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any information breaches;

6.2. To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to Personal Information;

6.3. To utilise information audits and risk assessments for mapping information and reducing the risk of breaches;

6.4. To have adequate and effective risk management procedures for assessing any risks presented by processing Personal Information;

6.5. To ensure that any Information Breaches are reported to the correct regulatory bodies within the timeframes;

6.6. To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring;

6.7. To use the Information Breach Incident Form for all information breaches, regardless of severity so that any patterns in causes can be identified and corrected;

6.8. To protect clients and staff – including their privacy, information and identity;

6.9. To ensure that where applicable, the Information Officer is involved in and notified about all Information Breaches; and

6.10. To ensure that the Information Regulator is notified of the Information Breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach.

7. INFORMATION BREACH PROCEDURES & GUIDELINES

7.1. Our procedures and guidelines for identifying, investigating and notification of Information Breaches are detailed below.

7.2. **Breach Monitoring & Reporting**

7.2.1. The Organisation has appointed an Information Officer who are responsible for the review and investigation of any Information Breach, regardless of the severity, impact or containment. All Information Breaches are reported to one of these persons with immediate effect, whereby the procedures detailed in this policy are followed.

7.2.2. All Information Breaches will be investigated, even in instances where notifications and reporting are not required, and We retain a full record of all information breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to an Information Breach, revision to any such process is recorded in the Organisation's policies.

7.3. **Breach Incident Procedures:**

7.3.1. **Identification of an Incident**

7.3.1.1. As soon as an Information Breach has been identified, it is reported to the direct line manager and the Information Officer immediately so that breach procedures can be initiated and followed without delay.

7.3.1.2. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Organisation. These procedures are for the protection of the Organisation, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

7.3.1.3. As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the Organisation, customer, client, third-party, system or information prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

7.3.2. **Breach Recording**

7.3.2.1. The Organisation utilises a Breach Incident Form for all incidents, which is completed for any Information Breach, regardless of severity or outcome. Completed forms are reviewed against existing records to ascertain patterns or reoccurrences.

7.3.2.2. In cases of Information Breaches, the Information Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

7.3.2.3. A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

7.3.2.4. The Information Regulator and the Data Subject(s) are notified in accordance with POPI requirements (refer to section 22 of POPI). In accordance with section 22, the notice to the Regulator shall be given without delay and the information stipulated in section 22(5) must be set out therein. In addition, any individual whose information or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

7.3.3. **Breach Risk Assessment**

7.3.3.1. **Human Error**

7.3.3.1.1. Where the Information Breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee held.

7.3.3.1.2. A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Organisation's risk assessment procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risks assessed to mitigate any future occurrence of the same root cause.

7.3.3.1.3. Resultant employee outcomes of such an investigation can include, but are not limited to: -

7.3.3.1.3. .7 Re-training in specific/all compliance areas;

7.3.3.1.3. .7 Re-assessment of compliance knowledge and understanding;

7.3.3.1.3. .7 Suspension from compliance related tasks; and/or

7.3.3.1.3.4. Formal warning (in-line with the Organisation's disciplinary procedures).

7.3.4. **System Error**

7.3.4.1. Where the Information Breach is the result of a system error/failure, the IT team are to work in conjunction with the Information Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

7.3.4.2. Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

7.3.4.2.1. Attempting to recover any lost equipment or Personal Information;

7.3.4.2.2. Shutting down an IT system;

7.3.4.2.3. Removing an employee from their tasks;

7.3.4.2.4. The use of back-ups to restore lost, damaged or stolen information;

7.3.4.2.5. Making the building secure;

7.3.4.2.6. If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed.

7.3.5. **Assessment of Risk and Investigation**

7.3.5.1. The Information Officer should ascertain what information was involved in the Information Breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

7.3.5.2. The Information Officer involved in the investigation should look at:

7.3.5.2.1. The type of information involved;

7.3.5.2.2. It's sensitivity or personal content;

7.3.5.2.3. What protections are in place (e.g. encryption)?

7.3.5.2.4. What happened to the information/Where is it now?

7.3.5.2.5. Whether there are any wider consequences/implications to the incident.

7.3.5.3. The appointed investigator should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

8. BREACH NOTIFICATIONS

8.1. The Organisation recognises its obligation and a duty to report Information Breaches in certain instances. All staff have been made aware of the Organisation's responsibilities and we have developed strict internal reporting lines to ensure that Information Breaches falling within the notification criteria are identified and reported without delay.

8.2. **Information Regulator Notification**

8.2.1. The Information Regulator is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual.

8.2.2. Where applicable, the Information Regulator is notified of the breach no later than 72 hours after us becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

8.2.3. If for any reason it is not possible to notify the Information Regulator of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay.

8.2.4. The notification to the Information Regulator will contain: -

8.2.4.1. A description of the likely consequences of the personal information breach;

8.2.4.2. A description of the measures taken or proposed to be taken to address the personal information breach (including measures to mitigate its possible adverse effects)

8.2.4.3. A recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the Information Breach;

8.2.4.4. If known to the Organisation, the identity of the unauthorized person who may have acquired access to Personal Information.

8.3. **Data Subject Notification**

8.3.1. When an Information Breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the Information Breach to the Data Subject without undue delay, in a written, clear and legible format.

8.3.2. The notification to the Data Subject shall include:

8.3.2.1. The nature of the Information Breach;

8.3.2.2. The name and contact details of our Information Officer and/or any other relevant point of contact (for obtaining further information);

8.3.2.3. A description of the likely consequences of the Information Breach;

8.3.2.4. A description of the measures taken or proposed to be taken to address the Information Breach (including measures to mitigate its possible adverse effects);

8.3.2.5. The identity of the perpetrator if known to the Organisation.

8.3.3. We reserve the right not to inform the Data Subject of any Personal Information Breach where we have implemented the appropriate technical and organisational protection measures which render the information unintelligible to any person who is not authorised to access it (i.e. encryption, information masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the Data Subject is no longer likely to materialise.

8.3.4. If informing the Data Subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the Data Subject(s) are informed in an equally effective manner.

9. RECORD KEEPING

9.1. All records and notes taking during the identification, assessment and investigation of the information breach are recorded and authorised by the Information Officer and are retained for a period of 5 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring**.**

10. RESPONSIBILITIES

10.1. The Organisation will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

10.2. The Information Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

INFORMATION BREACH INCIDENT FORM

INFORMATION OFFICER DETAILS:			
Name:	**Cobus Marais**	**Position:**	**Congregation Manager**
Date:		**Time:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			

WAS THE INFORMATION REGULATOR NOTIFIED?	**YES**	**NO**
IF YES, WAS THIS WITHIN 72 HOURS?	**YES**	**NO**
If no to the above, provide reason(s) for delay		
IF APPLICABLE, WAS THE BELOW INFORMATION PROVIDED?	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES**	**NO**
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE/S REVISED DUE TO BREACH:		

STAFF TRAINING PROVIDED: (if applicable)		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURRING AGAIN? (Describe)		
WERE APPROPRIATE TECHNICAL PROTECTION MEASURES IN PLACE?	**YES**	**NO**
If yes to the above, describe measures		
Information Officer Signature:		
Date:		

4.(POPI-4) DATA BREACH MANAGEMENT POLICY (for approval)

Final Audit Report 2021-06-29

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

"4.(POPI-4) DATA BREACH MANAGEMENT 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)
2021-06-29

Document signed by Roelof Jacobus Burger (roelf@skybegsol.co.za)
Signature Date: 2021-06-29

Agreement completed.
2021-06-29