FAMILIAE LEGATUM
PROTECT. GROW. CREATE.

An Authorised Financial Services Provider FSP 54212

POPIA COMPLIANCE POLICY

SIRIUS LEX
COMMITTED TO COMPLIANCE.

TABLE OF CONTENTS

1. THE AIM OF THE POPIA COMPLIANCE POLICY

1.1. **Background**

In terms of the FAIS Act, there is already a responsibility on all Financial Service Providers to ensure that data is kept safe, and in most cases for a period of 5 years after the relationship with the client has been terminated. In addition, POPIA is placing an additional level of data security on al entities to be adhered to.

1.2. **The aim of the POPIA Compliance Policy**

This policy aims to ensure that the FSP protects the clients' personal information, whilst adhering to all relevant legislation:

- FAIS
- FICA
- POPIA

1.3. **The principles of the POPIA Compliance Policy**

1. Data collection;
2. Data processing;
3. Data storage;
4. Data privacy;
5. Destruction of data (where and when applicable)

1.4. **The purpose of this document**

1. To ensure compliance with all the relevant legislation;
2. The aim is to focus on POPIA

2. KEY CONCEPTS

1. Develop, implement, monitor and maintain a compliance framework;
2. Perform personal information assessments;
3. Create awareness;
4. Ensure compliance;
5. Continuous Management

3. ROLES AND RESPONSIBILITIES

One person to be appointed to take full responsibility for this policy.

3.1. **Information Officer(s)**

- **Information Officer:** Elsje Niemann
- **Date of appointment:** 22 April 2024

** This is NOT the head of IT **
** This person has to be senior in the business**

This person takes full responsibility for the implementation of the POPIA compliance Policy.

3.2. **The role of all employees**

All employees will have to comply with this policy and everything related to POPIA.
Employees will have to identify PI and ensure that all measures are adhered to.

3.3. **The POPIA Policy and other Governance Risk and Compliance departments**
The POPIA policy is in line with the following internal policies of the FSP: Information Technology Governance

- **Information and Data Security**
- **Corporate Governance**
- **Compliance**
- **Risk Management**
- **Business Continuity Management)**
- **Conflict of Interest Management**
- **Treating Customers Fairly**

4. POLICY DEVELOPMENT, ALIGNMENT AND IMPLEMENTATION

A Financial Services Provider collects and processes Personal Information (PI) pertaining to their clients and for the purposes of advice given and financial services rendered. A client's consent needs to be obtained to collect and process his data – a completed application form and relevant compliance documents provides implied consent.

Examples of Personal Information collected includes, but is not limited to:

1. Name and Surname;
2. ID Number;
3. Address;
4. Employment details;
5. Salary details;
6. Bank details;
7. Medical History;
8. Dependent details;
9. Financial information;
10. Beneficiaries

It is advisable that a client is informed that the information collected will be kept for a period of 5 years after the relationship between the FSP and client has been terminated as per the FAIS Act requirements. FICA information is also required to be kept for a period of 5 years after termination.

Because of the above, data security is of the utmost importance. It is also vital to ensure that the FSP only retains data that is part of the transaction with the client.

The data security policy will form an essential part of the POPIA compliance policy and this document has to be updated as and when required. Data needs to be destroyed after 5 years following the termination date.

Penetration testing can be done to test data security on a regular basis.

Breach handling and escalation will be part of the responsibilities of the POPIA officer. A register of incidents will be kept with actions taken where applicable.

All employees will sign confidentiality agreements and non-disclosures.

Ensure that there is access control to all areas where data is kept. This includes strong passwords, no use of USB's or external hard drives allowed and building access control.

5. RISK ASSESSMENTS

Add POPIA to the Risk Management Plan as well as the Data Security Plan and update regularly.
Assess risks and breach incidents to establish the magnitude.

6. COMPLIANCE MONITORING

Policies will be monitored and updated on an annual basis.
Sampling will be done at regular intervals to test the Policy.

Consequences of non-compliance:

1. Warning;
2. Possible debarment;
3. Reporting of incidents to the relevant authorities;
4. Reporting of incidents to relevant clients
5. Possible sanctions and regulatory fines.

This Policy was accepted / implemented by Elsje Emerentia Niemann on 26 January **20** 26 **.**

Name / Surname Elsje Emerentia Niemann

Capacity **INFORMATION OFFICER**

Signature 

Name / Surname Martin Phillip Niemann

Capacity **WITNESS**

Signature