Camelot Wealth
(Pty)Ltd | FSP 54863 | Reg 2024/016417/07

Information Security & Data Safekeeping Policy

---

1. Introduction

Camelot Wealth (Pty) Ltd ("the Company") is entrusted with highly confidential client and business information. The safekeeping of such information is critical to maintaining client trust, meeting regulatory obligations, and protecting the integrity of the Company's operations.

This policy sets out the Company's standards, procedures, and responsibilities for safeguarding information in compliance with the Protection of Personal Information Act (POPIA), the Financial Advisory and Intermediary Services (FAIS) Act, and directives issued by the Financial Sector Conduct Authority (FSCA).

---

2. Purpose

The purpose of this policy is to:

- **Ensure the confidentiality, integrity, and availability of all client and business information.**
- **Define the security and safekeeping controls applied to both physical and electronic data.**
- **Provide employees with guidance on their responsibilities in handling information securely.**
- **Establish procedures for prevention, detection, and response to information security breaches.**

---

3. Scope

This policy applies to:

- **All employees, directors, key individuals, representatives, contractors, and service providers of the Company.**
- **All forms of information – including physical documents, electronic files, emails, databases, and communication records.**
- **All business processes where client and company data is collected, stored, processed, transmitted, or destroyed.**

---

4. Information Security Principles

The Company applies the following guiding principles to information management:

1. **Confidentiality – Information is only accessible to those who are authorised and who require it for legitimate business purposes.**
2. **Integrity – Information is accurate, complete, and safeguarded against unauthorised modification.**
3. **Availability – Information is accessible to authorised users when required, subject to proper safeguards.**

---

5. Safekeeping Controls

5.1 Physical Safeguards

- **All paper-based records are stored in locked cabinets in controlled-access areas.**
- **Only authorised staff may access physical files.**
- **Secure shredding is used for disposal of expired records.**

5.2 Electronic Safeguards

- **Data is stored on secure servers with firewalls, anti-virus protection, and encryption.**
- **Role-based access controls ensure staff only access information necessary for their role.**
- **Multi-factor authentication (MFA) is enabled for system access where available.**
- **Regular patching and security updates are applied to all systems.**

5.3 Backup & Continuity

- **Daily data backups are performed and stored in secure offsite or cloud environments.**
- **Backup systems are tested quarterly to ensure recoverability.**
- **The Company maintains a Business Continuity & Disaster Recovery Plan to ensure minimal disruption in case of system failures or disasters.**

5.4 Data Retention & Destruction

- **Records are retained in accordance with statutory requirements (minimum 5 years under FAIS, longer if prescribed by product providers or law).**
- **Once retention periods lapse, data is securely destroyed (shredding for paper, certified deletion for electronic data).**

5.5 Confidentiality & Sharing

- **All employees sign Confidentiality & POPIA Undertakings.**
- **Personal Information is only shared with third parties where lawful and with client consent.**

- **Strict vendor due diligence is applied before sharing data with service providers.**

5.6 Monitoring & Incident Response

- **All access to sensitive client data is logged and monitored.**
- **Suspected or confirmed data breaches must be reported immediately to the Information Officer.**
- **The Company will notify the FSCA and affected clients of breaches where required by law.**

---

6. Roles and Responsibilities

- **Board of Directors / Key Individuals**
  - **Provide oversight and ensure adequate resources for information security.**
- **Information Officer (appointed under POPIA)**
  - **Oversees compliance with POPIA and FSCA requirements.**
  - **Acts as the central point for breach notifications.**
- **Compliance Officer**
  - **Monitors adherence to this policy and reports findings to management.**
- **All Employees & Representatives**
  - **Must handle information responsibly, safeguard access credentials, and report any suspected breaches.**

---

7. Training & Awareness

- **Information security and POPIA compliance are included in induction training.**
- **Refresher training is provided annually, including updates on new threats and regulatory requirements.**
- **Employees are regularly reminded of the importance of password hygiene, phishing awareness, and confidentiality.**

---

8. Policy Review

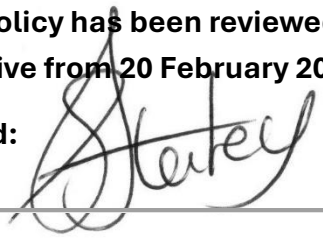
This policy is reviewed annually or when regulatory, business, or technological changes necessitate amendments.

---

9. Approval

This policy has been reviewed and approved by the Board of Camelot Wealth (Pty) Ltd and is effective from 20 February 2025.

Signed:



Director / Key Individual

Date: 20/02/2025