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

Procedures for Safekeeping of Information

1. Purpose

To ensure all client and company information is safeguarded in compliance with the POPI Act, FAIS Act, and FSCA requirements, and to protect against loss, unauthorised access, alteration, or disclosure.

---

2. Safekeeping Procedures

a) Physical Security

- **All paper records are stored in locked cabinets in restricted-access areas.**
- **Only authorised staff have keys/access to filing rooms.**
- **Visitors are not permitted in record storage areas without supervision.**

b) Electronic Security

- **Client data is stored on secure, password-protected servers with firewalls and encryption.**
- **Access is role-based (only staff who need the data can access it).**
- **Passwords must be changed every 60–90 days and must meet strong complexity standards.**
- **Multi-factor authentication (MFA) is enabled for system access.**

c) Data Back-Up & Continuity

- **Daily backups are performed and stored securely offsite or in a secure cloud.**
- **Business continuity plans (BCP) ensure access to records in case of system failures or disasters.**
- **Backup recovery procedures are tested quarterly.**

d) Confidentiality Controls

- **All employees sign a Confidentiality & POPIA Undertaking.**
- **Client information is only shared with third parties where lawful and with client consent.**
- **POPIA-compliant consent forms are retained in client files.**

e) Document Retention & Destruction

- **Records are retained in line with statutory requirements (e.g., 5 years under FAIS).**
- **Secure shredding of physical files and certified deletion of electronic data after the retention period.**

f) Monitoring & Incident Management

- **All access to client files is logged and monitored.**
- **Breaches or suspected breaches are reported immediately to the Information Officer.**
- **Clients and regulators are notified where required under POPIA breach notification rules.**

---

3. Roles and Responsibilities

- **Information Officer: Oversees compliance with POPIA and FSCA recordkeeping rules.**
- **Compliance Officer: Monitors implementation of controls and reports breaches.**
- **All Staff: Responsible for safeguarding information entrusted to them.**

---

4. Review

These procedures are reviewed annually or when there are material regulatory or operational changes.

This forms part of your Compliance & POPIA framework, and you can expand it into a full Information Security Policy if required.