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

POPI Information Safekeeping Procedures

---

1. Purpose

To ensure that all personal, financial, and confidential information handled by Camelot Wealth (Pty) Ltd is protected against unauthorised access, loss, misuse, or disclosure, and that client trust and regulatory compliance are maintained.

---

2. Scope

These procedures apply to:

- **All employees, directors, representatives, and contractors.**
- **All types of information (electronic, paper, voice recordings, email, cloud storage).**
- **All stages of information handling (collection, storage, processing, transfer, and destruction).**

---

3. Safekeeping Procedures

3.1 Physical Information Security

- **Client files are stored in locked cabinets in restricted-access areas.**
- **Only authorised staff may access filing rooms or cabinets.**
- **Visitors are not permitted in confidential areas without supervision.**
- **Hard copy records due for disposal are shredded using secure shredding facilities.**

3.2 Electronic Information Security

- **All systems are password-protected with multi-factor authentication (MFA) where available.**
- **Access is role-based, granting only the minimum information required for job functions.**
- **Data is stored on servers with encryption, firewalls, and anti-virus protection.**
- **Remote access is secured via VPN and monitored.**

- **Audit logs are kept of all access to sensitive data.**

3.3 Back-Up and Business Continuity

- **Daily automated backups of electronic records are performed and stored securely in an offsite/cloud location.**
- **Backups are tested quarterly to ensure recoverability.**
- **A Business Continuity & Disaster Recovery Plan (BCP) ensures access to information in case of fire, theft, or system failure.**

3.4 Confidentiality and Non-Disclosure

- **All employees sign a Confidentiality & POPIA Undertaking.**
- **Client information is only shared with third parties where required by law or with written client consent.**
- **Sensitive information (e.g., medical records, banking details) is restricted to authorised users only.**

3.5 Data Retention & Destruction

- **Information is retained in line with FSCA and FAIS requirements (minimum 5 years).**
- **Expired records are destroyed using secure shredding or digital wiping tools.**
- **A Retention & Destruction Register is maintained.**

3.6 Monitoring & Breach Management

- **All access to client data is monitored and logged.**
- **Any suspected or actual data breach must be reported immediately to the Information Officer.**
- **The Information Officer will assess, contain, and, if required, notify the Information Regulator and affected clients.**

---

4. Roles and Responsibilities

- **Board of Directors/Key Individuals – overall accountability for information protection.**
- **Information Officer (appointed under POPIA) – ensures compliance, breach reporting, and monitoring.**
- **Compliance Officer – reviews adherence and maintains oversight.**
- **All Staff – responsible for safeguarding any information they access or handle.**

---

5. Training and Awareness

- **All employees receive induction training on information security and POPIA.**

- **Refresher training is provided annually.**
- **Regular staff awareness campaigns reinforce best practices (e.g., password hygiene, phishing awareness).**

---

6. Review

These procedures were reviewed on 20 February 2025 and are reviewed annually or when changes in legislation, business operations, or technology occur.
