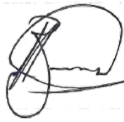


### Policy Review Control Sheet

|                                           |                                                                         |         |
|-------------------------------------------|-------------------------------------------------------------------------|---------|
| <b>Governance Area</b>                    | Technology, Data & Information Governance (as per Governance Framework) |         |
| <b>Policy Name</b>                        | Promotion of Access to Information Policy (PAIA)                        |         |
| <b>Policy Owner (FSP) &amp; Version #</b> | GNT CAPITAL (PTY) LTD                                                   | 1       |
| <b>Original &amp; Previous approval</b>   |                                                                         | N/A     |
| <b>Review Frequency &amp; Month</b>       | Annually                                                                | October |
| <b>Next Review Date &amp; Month</b>       | 2027                                                                    | October |

### Policy Review Details

|                                     |                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------|
| <b>Date of Review</b>               | 8th of October 2026                                                                 |
| <b>Reviewer Name(s)</b>             | HENDRIK BENJAMIN BARNARD                                                            |
| <b>Summary of Changes</b>           | N/A                                                                                 |
| <b>Reason for Changes</b>           |                                                                                     |
| <b>Approval Status</b>              | Approved                                                                            |
| <b>Approved By<br/>Signature(s)</b> |  |
| <b>Approval Date</b>                | 8/10/2026                                                                           |

### Change Log

| <b>Date</b> | <b>Change Description</b> | <b>Changed By</b> | <b>Version #</b> |
|-------------|---------------------------|-------------------|------------------|
|             |                           |                   |                  |
|             |                           |                   |                  |

Training & Implementation

|                 |                            |
|-----------------|----------------------------|
| <b>Planning</b> | <b>Responsible Person:</b> |
|                 |                            |
|                 |                            |
|                 |                            |

Confirmation of Training & Implementation

|                                                                                      |                            |
|--------------------------------------------------------------------------------------|----------------------------|
| <b>Confirmation</b>                                                                  | <b>Responsible Person:</b> |
| <b>Date, Time, Attendees, Presentation recorded in the Inhouse Training Register</b> |                            |
|                                                                                      |                            |
|                                                                                      |                            |

**GNT CAPITAL (PTY) LTD's**  
**PROMOTION OF ACCESS TO INFORMATION**  
**ACT (PAIA) POLICY**

## **Table of Contents**

1. Policy Purpose and Objectives
  2. Scope and Applicability
  3. Regulatory Framework
  4. Definitions
  5. Governance and Accountability
  6. PAIA Manual Requirements
  7. Categories of Records Held by the FSP
  8. Automatically Available Records
  9. PAIA Request Procedure
  10. Statutory Timelines and Extensions
  11. Grounds for Refusal or Partial Refusal
  12. Third-Party Information and Consultation
  13. POPIA Alignment and Data Subject Requests
  14. Fees
  15. Secure Disclosure and Redaction Standards
  16. Recordkeeping and Evidence Pack
  17. PAIA Registers
  18. Annual PAIA Reporting and Information Regulator Engagement
  19. Training and Awareness
  20. Outsourcing, Operators and Product Suppliers
  21. Non-Compliance and Disciplinary Consequences
  22. Monitoring, Assurance and Review
- Appendix A: PAIA Request Intake Checklist
- Appendix B: PAIA Decision Checklist
- Appendix C: Template Acknowledgement Letter
- Appendix D: Template Decision Letter – Grant / Partial Grant / Refusal
- Appendix E: PAIA Request Register Template
- Appendix F: Minimum PAIA Manual Customization Schedule
- Appendix G: Source and Guidance Notes for Customization

## **1. Policy Purpose and Objectives**

This PAIA Policy establishes the governance, responsibilities, controls and procedures through which GNT CAPITAL (PTY) LTD (“the FSP”, “the Company”, “we”, “us” or “our”) complies with the Promotion of Access to Information Act, 2 of 2000 (“PAIA”), as amended, and related obligations under the Protection of Personal Information Act, 4 of 2013 (“POPIA”).

- Give effect to the constitutional right of access to information in a lawful, transparent and accountable manner.
- Ensure requesters can identify records held by the FSP and understand how to request access.
- Ensure access requests are received, validated, assessed, decided and responded to within statutory timeframes.
- Balance access to information with the protection of privacy, confidential information, privileged information, commercial interests, regulatory restrictions and the rights of third parties.
- Align PAIA processes with FSP-specific obligations under FAIS, FSCA conduct standards, FIC Act recordkeeping, complaints management, data protection and information security requirements.
- Maintain a current PAIA Manual and supporting operational records, registers, templates and evidence packs.
- Support annual PAIA reporting, Information Officer accountability, staff awareness and continuous improvement.

## **2. Scope and Applicability**

This Policy applies to all directors, key individuals, representatives, employees, temporary staff, contractors, outsourced service providers and any other persons who create, receive, access, process, store, disclose, archive or destroy records for or on behalf of the FSP.

- All records in any form, including paper, electronic, audio, visual, messaging, cloud-hosted, outsourced and archived records.
- All business units and functions, including advice, intermediary services, investments, insurance, retirement benefits, administration, finance, HR, compliance, risk, IT, sales, marketing and complaints.
- All PAIA requests received from clients, prospective clients, employees, former employees, regulators, attorneys, beneficiaries, claimants, product suppliers, business partners or members of the public.
- All POPIA requests for access to personal information, correction, deletion or objection, where processed through the PAIA/POPIA rights-management process.

### 3. Regulatory Framework

The FSP must interpret and apply this Policy consistently with the following legislative and regulatory instruments, as amended from time to time:

| Instrument                                                                                          | Relevance to this Policy                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Constitution of the Republic of South Africa, 1996</b>                                           | Section 32 establishes the right of access to information held by the state and information held by another person required for the exercise or protection of rights; section 14 protects privacy. |
| <b>Promotion of Access to Information Act, 2 of 2000 (PAIA)</b>                                     | Primary statute governing access to records of public and private bodies, requester procedures, grounds for refusal, third-party notification, fees, internal/external remedies and manuals.       |
| <b>PAIA Regulations and prescribed forms</b>                                                        | Prescribed request, appeal/complaint and fee mechanisms, including Form 2 for access requests and applicable fee rules.                                                                            |
| <b>Protection of Personal Information Act, 4 of 2013 (POPIA)</b>                                    | Regulates lawful processing of personal information and establishes Information Officer responsibilities; PAIA is the mechanism for access to records containing personal information.             |
| <b>Financial Advisory and Intermediary Services Act, 37 of 2002 (FAIS) and subordinate measures</b> | Requires FSPs, Key Individuals and Representatives to maintain proper client, advice, disclosure, complaints, conflict of interest, competency and compliance records.                             |
| <b>Financial Sector Regulation Act, 9 of 2017 (FSR Act)</b>                                         | Establishes Twin Peaks regulatory architecture and the FSCA's market conduct role.                                                                                                                 |
| <b>Financial Intelligence Centre Act, 38 of 2001 (FIC Act)</b>                                      | Imposes customer due diligence, accountable institution, suspicious transaction reporting and AML/CFT recordkeeping obligations where applicable.                                                  |
| <b>Companies Act, 71 of 2008 and CIPC requirements</b>                                              | Company governance, statutory records and corporate disclosure requirements.                                                                                                                       |
| <b>Electronic Communications and Transactions Act, 25 of 2002</b>                                   | Electronic records, data messages, electronic communications and related validity/retention considerations.                                                                                        |
| <b>Labour legislation including BCEA, LRA, EEA and OHSA</b>                                         | Employment, HR, payroll, health and safety and workplace records.                                                                                                                                  |

|                                                           |                                                                                         |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Tax Administration Act, VAT Act and Income Tax Act</b> | Tax, accounting and audit records and retention duties.                                 |
| <b>Common law, legal privilege and contract</b>           | Confidentiality, privilege, fiduciary duties and contractual nondisclosure obligations. |

#### 4. Definitions

| <b>Term</b>                             | <b>Meaning</b>                                                                                                                                              |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access fee</b>                       | The prescribed fee payable by a requester for the reproduction, search, preparation and delivery of records, where applicable.                              |
| <b>Data subject</b>                     | The person to whom personal information relates, as defined in POPIA.                                                                                       |
| <b>Deputy Information Officer (DIO)</b> | A person designated to assist the Information Officer with PAIA and POPIA responsibilities.                                                                 |
| <b>Head of private body</b>             | For a private body, the person contemplated in PAIA as responsible for compliance, typically the CEO, managing director, sole proprietor or equivalent.     |
| <b>Information Officer (IO)</b>         | The person who bears overall responsibility for PAIA/POPIA compliance within the FSP, including the PAIA Manual, access requests and regulatory engagement. |
| <b>Personal information</b>             | Information relating to an identifiable natural or juristic person as defined in POPIA.                                                                     |
| <b>Private body</b>                     | A natural person, partnership, juristic person or former/existing juristic person carrying on trade, business or profession.                                |
| <b>Record</b>                           | Any recorded information, regardless of form or medium, in the possession or under the control of the FSP, whether or not created by the FSP.               |
| <b>Requester</b>                        | Any person making a request for access to a record, including a personal requester seeking their own personal information.                                  |
| <b>Third party</b>                      | Any person other than the requester and the FSP whose information or rights may be affected by the request.                                                 |

## 5. Governance and Accountability

| Role                                              | PAIA responsibilities                                                                                                                                                         |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Board / Governing Body / Owner</b>             | Approve this Policy and PAIA Manual; set compliance tone; ensure adequate resources; receive material PAIA/POPIA compliance reporting.                                        |
| <b>Key Individual(s)</b>                          | Ensure PAIA controls are embedded in the FSP's FAIS governance framework and that representatives cooperate with record searches and client rights.                           |
| <b>Information Officer / Head of Private Body</b> | Own PAIA compliance; register with the Information Regulator where required; maintain PAIA Manual; make or approve access decisions; ensure reporting and evidence retention. |
| <b>Deputy Information Officer(s)</b>              | Operationally administer requests, maintain registers, coordinate searches, communicate with requesters and third parties, prepare decision letters and escalate risks.       |
| <b>Compliance Officer</b>                         | Monitor compliance, advise on regulatory requirements, conduct periodic reviews, test evidence, update templates and report control weaknesses.                               |
| <b>Records / Data Owners</b>                      | Identify, retrieve and validate records; confirm retention status; classify sensitivity; assist with redaction and disclosure decisions.                                      |
| <b>IT / Information Security</b>                  | Support searches of electronic systems, logs, backups and archives; preserve records; implement access controls; support secure disclosure.                                   |
| <b>Employees and Representatives</b>              | Promptly forward PAIA requests to the DIO/IO; maintain accurate records; preserve confidentiality; complete awareness training.                                               |
| <b>Outsourced Service Providers / Operators</b>   | Assist with searches and retrieval in accordance with contracts, POPIA operator clauses and information-security requirements.                                                |

## 6. PAIA Manual Requirements

The FSP must maintain a current PAIA Manual prepared in terms of PAIA section 51 and aligned to the Information Regulator's template and guidance. The Manual is a public-facing document and must be sufficiently clear to enable requesters to understand the FSP's records and how to access them.

The PAIA Manual must include, at a minimum:

- Company details: registered name, registration number, FSP number, business address, postal address, website and contact channels.
- Information Officer and Deputy Information Officer contact details.
- Reference to the Information Regulator's guide on how to use PAIA and how it can be obtained.
- A description of categories of records that are automatically available without a formal PAIA request.
- A description of records available in accordance with other legislation.
- A description of subjects and categories of records held by the FSP.
- Processing of personal information, including purposes, categories of data subjects, categories of personal information, recipients, cross-border transfers and security safeguards.
- How to submit a PAIA request, including prescribed forms, identity requirements, fees and available assistance.
- Grounds for refusal and remedies available to requesters.
- Manual availability, languages, locations and update frequency.

The Manual must be available on the FSP's website, at the FSP's principal place of business and by request from the IO/DIO. Where appropriate, the FSP should make the Manual available in English and any additional official language(s) reasonably relevant to its client base and operations.

## 7. Categories of Records Held by the FSP

| Subject                                 | Examples of record categories                                                                                                                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Corporate and governance</b>         | Company registration documents, constitutional documents, shareholder/member records, board minutes, delegation of authority, policies, risk registers, compliance reports, statutory returns.    |
| <b>FAIS licensing and regulatory</b>    | FSP licence, licence conditions, FSCA correspondence, KI and representative register, fit and proper evidence, CPD records, compliance monitoring reports, regulatory returns, debarment records. |
| <b>Client onboarding and KYC</b>        | Application forms, mandates, FICA/CDD records, risk ratings, sanctions/PEP screening evidence, source of funds/wealth, beneficial ownership records, consent records.                             |
| <b>Advice and intermediary services</b> | Needs analyses, records of advice, product comparisons, quotes, disclosures, replacement advice, suitability assessments, product supplier correspondence, transaction instructions.              |

|                                                 |                                                                                                                                                                     |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Investment / insurance / product records</b> | Policy schedules, investment statements, claims records, beneficiary nominations, premium/contribution records, portfolio data, product supplier data feeds.        |
| <b>Complaints and dispute resolution</b>        | Complaints register, complaint files, investigation notes, outcomes, Ombud correspondence, root-cause analysis and TCF/market conduct remediation evidence.         |
| <b>Financial and tax</b>                        | Accounting records, invoices, bank statements, commission statements, payroll, tax filings, audit files, budgets and management accounts.                           |
| <b>Human resources</b>                          | Employment contracts, personnel files, performance records, disciplinary records, leave records, training and competence records, remuneration and benefit records. |
| <b>Information technology and security</b>      | User access records, system logs, backups, asset registers, incident records, vulnerability reports, vendor assessments, cyber policies.                            |
| <b>Marketing and communications</b>             | Campaigns, consent/opt-out records, client communications, website content, social media governance, lead sources.                                                  |
| <b>Contracts and suppliers</b>                  | Service-level agreements, outsourced arrangements, operator agreements, due diligence, confidentiality agreements, procurement records.                             |
| <b>Legal and litigation</b>                     | Legal opinions, privileged communications, contracts, claims, subpoenas, settlement agreements, regulatory investigations.                                          |

## 8. Automatically Available Records

Certain information may be made available without requiring a formal PAIA request. The DIO must maintain a schedule of automatically available records and review it at least annually.

- Public website information, brochures, product disclaimers and general contact details.
- PAIA Manual and privacy notice.
- FSP license details that are publicly available through FSCA channels.
- Publicly available company information and statutory information that the FSP has elected to publish.
- Generic complaints procedure and conflict of interest policy summary, where published.
- Any other records identified in the PAIA Manual as automatically available.

## 9. PAIA Request Procedure

All PAIA requests must be handled centrally by the IO/DIO. Staff must not independently approve, reject, disclose or destroy records once a request is received.

| Step                                       | Control requirement                                                                                                                                                              |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Receipt</b>                          | Receive the request via prescribed Form 2 or another written channel. If a request is informal but appears to seek access under PAIA/POPIA, forward it to the DIO immediately.   |
| <b>2. Log and acknowledge</b>              | Record the request in the PAIA Request Register within 1 business day and acknowledge receipt, noting any missing information, identity documents, authority or fees.            |
| <b>3. Validate requester and authority</b> | Confirm identity for personal requesters and legal authority for representatives, attorneys, guardians, executors, employers or corporate requesters.                            |
| <b>4. Clarify scope</b>                    | If the request is vague, assist the requester to describe the record sufficiently. Do not use clarification to delay unreasonably.                                               |
| <b>5. Assess fees</b>                      | Determine whether request fees and/or access fees apply. Personal requesters seeking their own personal information should not be charged a request fee where exempt under PAIA. |
| <b>6. Search and preserve</b>              | Issue a legal/records hold where necessary and coordinate searches across relevant systems, custodians, archives and service providers.                                          |
| <b>7. Review records</b>                   | Assess whether the requested records exist, are under the FSP's control, are subject to any statutory grounds for refusal, require redaction, or implicate third-party rights.   |
| <b>8. Third-party notification</b>         | Notify affected third parties where PAIA requires consultation and allow representations before deciding.                                                                        |
| <b>9. Decision</b>                         | The IO/DIO prepares a written decision to grant, partially grant, refuse, transfer or defer access, with reasons and remedies.                                                   |
| <b>10. Secure disclosure</b>               | Provide records in the approved format after applicable fees are paid, using secure channels and minimum necessary disclosure.                                                   |
| <b>11. Close and retain evidence</b>       | Update the register, retain the request file, decision rationale, copies disclosed/refused, correspondence, fee evidence and review lessons learned.                             |

## **10. Statutory Timelines and Extensions**

- The FSP must respond to a PAIA request as soon as reasonably possible and within the statutory period prescribed by PAIA, generally 30 calendar days after receipt of a valid request.
- An extension may be taken only where PAIA permits it, including where the request is for a large number of records, requires searches at another location, requires consultation, or cannot reasonably be completed within the original period.
- Any extension notice must be issued before the original deadline expires, state the period of extension, reasons and available remedies.
- If the FSP fails to respond within the required period, this may be treated as a deemed refusal and may trigger complaint/escalation rights.

## 11. Grounds for Refusal or Partial Refusal

Access may only be refused where PAIA permits or requires refusal. The IO/DIO must document the applicable ground, evidence and balancing considerations. Where a ground applies only to part of a record, the FSP must consider redaction and partial disclosure.

| Ground                                                                            | Policy application                                                                                                                                    |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mandatory protection of privacy</b>                                            | Personal information of third parties may not be disclosed unless PAIA/POPIA permits disclosure or the third-party consents.                          |
| <b>Commercial information of third parties</b>                                    | Trade secrets, financial, commercial, scientific or technical information that could cause harm to a third party's commercial or financial interests. |
| <b>Confidential information</b>                                                   | Information supplied in confidence where disclosure would breach a duty of confidence or prejudice future supply of similar information.              |
| <b>Safety and security</b>                                                        | Information whose disclosure could endanger life, physical safety, security systems or property.                                                      |
| <b>Legal privilege</b>                                                            | Records protected by legal professional privilege unless privilege is waived.                                                                         |
| <b>Commercial information of the FSP</b>                                          | Trade secrets, commercial information, proprietary methods, pricing, strategies or confidential business information of the FSP.                      |
| <b>Research information</b>                                                       | Research information where disclosure would expose the FSP, third party or researcher to serious disadvantage.                                        |
| <b>Manifestly frivolous or vexatious / substantial and unreasonable diversion</b> | Requests that meet PAIA's threshold for refusal based on abuse or disproportionate burden must be handled cautiously and with documented reasons.     |

## **12. Third-Party Information and Consultation**

- The DIO must identify whether a requested record contains personal information, confidential information, commercial information or other protected information relating to a third party.
- Where required, the FSP must notify the third party and provide a reasonable opportunity to make representations or consent to disclosure.
- The IO/DIO must consider third-party representations objectively but must make the final decision in accordance with PAIA.
- If access is granted despite third-party objection, the FSP must follow PAIA notice requirements and allow the third party to exercise available remedies before release where applicable.

## **13. POPIA Alignment and Data Subject Requests**

PAIA and POPIA must be applied together. A request by a data subject for access to their personal information must be handled through the PAIA/POPIA rights-management process, with due regard to identity verification, security, third-party rights and applicable exemptions.

- The FSP must maintain privacy notices explaining purposes of processing, categories of data subjects, information processed, recipients, cross-border transfers, safeguards and rights.
- The FSP must only disclose personal information through secure channels and only to the verified requester or authorized representative.
- Requests for correction, deletion, destruction, objection or withdrawal of consent must be escalated to the POPIA procedure and recorded in the Data Subject Request Register.
- Where records must be retained under FAIS, FIC Act, tax, employment or other laws, deletion requests may be refused or limited with reasons.
- Security compromises discovered during PAIA handling must be escalated under the Incident Response and POPIA Breach Notification procedure.

## **14. Fees**

- The DIO must apply only the fees permitted by PAIA and the current regulations.
- A requester must be notified in writing of any fee payable, calculation method and payment process.
- Access to records may be withheld until applicable access fees are paid, where PAIA permits this.
- Fee decisions must be recorded in the PAIA Request Register and evidence of payment retained.
- The FSP may waive fees where the cost of collection exceeds the fee, where required by law or where approved by the IO in exceptional circumstances.

## 15. Secure Disclosure and Redaction Standards

- Disclose only the record or portion of the record approved for release.
- Redact exempt information permanently using secure redaction tools; do not rely on formatting, highlighting or hidden text.
- Label disclosed records as “PAIA disclosure copy” where appropriate and retain a copy of the disclosed version.
- Use secure delivery methods such as encrypted email, secure portal, password-protected file transfer, registered courier or in-person collection with identity verification.
- Record the disclosure date, method, recipient and any password/transmission controls in the request file.

## 16. Recordkeeping and Evidence Pack

For each PAIA request, the DIO must maintain an evidence pack sufficient to demonstrate compliance.

The evidence pack must include:

- Original request and prescribed form, if applicable.
- Requester identity and authority verification evidence.
- Acknowledgement, clarification, fee and extension correspondence.
- Search instructions, search results and custodians consulted.
- Copies of records located and the approved redacted disclosure copy.
- Refusal/partial refusal legal assessment and decision rationale.
- Third-party notices, representations and decisions.
- Final response, proof of delivery and payment evidence.
- Escalations, complaints, regulator interactions and lessons learned.

## 17. PAIA Registers

The FSP must maintain, at minimum, the following registers:

| Register                                 | Minimum content                                                                                 |
|------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>PAIA Request Register</b>             | All access requests, status, deadlines, decisions, fees, disclosure method and closure details. |
| <b>Third-Party Consultation Register</b> | Third parties notified, response deadlines, representations, outcome and release status.        |
| <b>Data Subject Request Register</b>     | POPIA access, correction, deletion, objection and consent withdrawal requests.                  |

|                                                 |                                                                    |
|-------------------------------------------------|--------------------------------------------------------------------|
| <b>Automatically Available Records Schedule</b> | Records available without formal request and publication location. |
| <b>PAIA Manual Review Register</b>              | Version history, review dates, approvals and publication evidence. |
| <b>Training and Awareness Register</b>          | Staff training dates, attendees, modules and assessment evidence.  |

## 18. Annual PAIA Reporting and Information Regulator Engagement

- The IO/DIO must monitor Information Regulator notices and submit annual PAIA reporting when required through the Regulator's prescribed channel or eServices portal.
- The FSP must keep an annual summary of PAIA requests received, granted, partly granted, refused, transferred, withdrawn, pending, appealed/complained about and otherwise closed.
- Any communication, complaint, enforcement notice or request from the Information Regulator must be escalated immediately to the IO, Compliance Officer and governing body where material.
- The FSP must retain proof of PAIA Manual publication, Information Officer registration, PAIA reporting and any submissions to the Regulator.

## 19. Training and Awareness

- All employees and representatives must receive PAIA/POPIA awareness appropriate to their roles at onboarding and at least annually thereafter.
- Training must explain how to recognize PAIA requests, where to forward them, confidentiality duties, record preservation, redaction risks and escalation requirements.
- High-risk roles such as client services, complaints, advisers, HR, IT, compliance and management must receive enhanced training.  
Training completion must be recorded and non-completion escalated.

## 20. Outsourcing, Operators and Product Suppliers

- Contracts with administrators, cloud providers, CRM providers, compliance practices, product suppliers, brokers, binder holders, claims administrators and other service providers must require cooperation with PAIA/POPIA requests.
- Contracts must address confidentiality, security, access to records, return/destruction of records, audit rights, breach notification and cross-border processing where relevant.
- The FSP remains accountable for records under its control even where records are held by an outsourced service provider.
- The DIO must maintain contact points and service-level expectations for urgent record searches.

## 21. Non-Compliance and Disciplinary Consequences

- Failure to comply with this Policy may expose the FSP to regulatory action, enforcement notices, penalties, litigation, client harm, reputational damage and FSCA conduct risk.
- Employees who fail to escalate requests, disclose records without authority, alter or destroy records, obstruct searches or breach confidentiality may face disciplinary action.
- Material breaches must be reported to the IO, Compliance Officer and governing body and, where required, to the Information Regulator, FSCA or other regulator.

## 22. Monitoring, Assurance and Review

- The Internal Compliance Officer must review this Policy and the PAIA Manual at least annually and when laws, regulations, business activities, records, systems or regulator guidance change.
- Periodic testing should include sample request files, deadline compliance, register completeness, manual availability, staff awareness, redaction controls and outsourced-service-provider responsiveness.
- Findings must be recorded in a compliance monitoring report with responsible persons, actions and due dates.
- The governing body or authorized governance forum must approve material amendments.

## Appendix A: PAIA Request Intake Checklist

| Control                                                         | Done                     |
|-----------------------------------------------------------------|--------------------------|
| Request received date and channel captured                      | <input type="checkbox"/> |
| Request forwarded to DIO/IO within 1 business day               | <input type="checkbox"/> |
| Prescribed request form received or requester assisted          | <input type="checkbox"/> |
| Identity verified                                               | <input type="checkbox"/> |
| Authority / mandate verified where request is by representative | <input type="checkbox"/> |
| Requested record sufficiently described                         | <input type="checkbox"/> |
| Requester type confirmed: personal / non-personal / third party | <input type="checkbox"/> |
| Fees assessed and notice issued if applicable                   | <input type="checkbox"/> |
| Deadline calculated and diarised                                | <input type="checkbox"/> |
| Relevant custodians and systems identified                      | <input type="checkbox"/> |
| Record hold issued if required                                  | <input type="checkbox"/> |
| Third-party consultation assessed                               | <input type="checkbox"/> |

## **Appendix B: PAIA Decision Checklist**

- Does the record exist and is it in the FSP's possession or under its control?
- Is the requester entitled to the record without a formal request because it is automatically available?
- Does the record contain personal information of the requester only?
- Does the record contain third-party personal, confidential or commercial information?
- Does legal privilege apply?
- Does any statutory ground for refusal apply, and is it mandatory or discretionary?
- Can exempt information be severed/redacted so that the remainder can be disclosed?
- Have all required third-party notices and representations been handled?
- Have fees been calculated and communicated correctly?
- Does the response letter include reasons, remedies and the correct disclosure/refusal details?
- Has the disclosed version been securely redacted and quality-checked?

## **Appendix C: Template Acknowledgement Letter**

[Date]

[Requester name]

[Address / email]

Dear [Requester name],

### **ACKNOWLEDGEMENT OF REQUEST FOR ACCESS TO RECORDS**

We acknowledge receipt of your request dated [date] for access to [brief description of records]. Your request reference number is [reference]. We are assessing the request in terms of PAIA and, where relevant, POPIA. We may contact you for clarification, proof of identity, authority or payment of prescribed fees. A decision will be communicated within the statutory timeframe, subject to any permitted extension.

Yours faithfully,

[Name]

[Information Officer / Deputy Information Officer]

## **Appendix D: Template Decision Letter – Grant / Partial Grant / Refusal**

[Date]

[Requester name]

[Address / email]

Dear [Requester name],

DECISION ON REQUEST FOR ACCESS TO RECORDS: [REFERENCE]

We refer to your request dated [date]. After considering the request and the records identified, our decision is as follows:

- Decision: [Granted / Partially granted / Refused / Transferred / Deferred].
- Records covered by this decision: [describe records].
- Reasons: [provide concise reasons, including applicable PAIA provisions or considerations].
- Redactions: [describe categories of information redacted and reasons].
- Fees payable: [amount / not applicable].
- Access method: [secure email / collection / courier / inspection / other].
- Remedies: You may lodge a complaint with the Information Regulator or approach a court, as provided for in PAIA.

Yours faithfully,

[Name] [Information Officer / Deputy Information Officer]

## Appendix E: PAIA Request Register Template

| Ref                   | Received | Requester | Record requested | Due date   | Decision                | Fees         | Closed | Notes       |
|-----------------------|----------|-----------|------------------|------------|-------------------------|--------------|--------|-------------|
| PAIA-<br>YYYY<br>-001 | [date]   | [name]    | [summary<br>]    | [date<br>] | [grant/refuse/etc.<br>] | [amount<br>] | [date] | [notes<br>] |

## Appendix F: Minimum PAIA Manual Customization Schedule

| Area                            | Client-specific detail required                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------|
| Client identity                 | Registered name, trading name, company registration number, FSP number and license categories. |
| Contact details                 | Physical, postal, telephone, website and dedicated PAIA/POPIA email address.                   |
| IO/DIO details                  | Names, titles, contact details, registration status and delegations.                           |
| Record map                      | Client-specific records held by function, system, outsourced provider and retention period.    |
| Automatically available records | List and access location.                                                                      |
| Personal information processing | Data subjects, data categories, purposes, recipients, cross-border transfers and safeguards.   |
| Languages and publication       | Website link, office copy and language versions appropriate to the client base.                |
| Approvals                       | Board/KI/owner approval and version history.                                                   |