PROMOTION OF ACCESS TO INFORMATION ACT (PAIA) MANUAL

Prepared in terms of Section 51 of the Promotion of Access to Information Act, 2 of 2000, as amended, and aligned to POPIA governance requirements.

Field	Detail
Document Reference	KAIROS-PAIA
Organisation	Kairos Computer Risk Management
Classification	Public / External
Version	2.0
Status	Approved / Active
Approved By	Gary Grant Adams, CTIO
Approval Date	17 October 2025
Effective Date	21 October 2025
Next Review Date	21 October 2026
Information Officer	Gary Grant Adams

Table of Contents

1. Introduction

1.1 Purpose of this Manual

1.1.1 This PAIA Manual explains how members of the public, clients, employees, contractors, suppliers, data subjects and other requesters may request access to records held by Kairos Computer Risk Management ("Kairos").

1.1.2 This Manual supports transparency, lawful access to records, and responsible handling of personal information and confidential information.

1.2 Legal Basis

1.2.1 This Manual is prepared in terms of Section 51 of the Promotion of Access to Information Act, 2 of 2000 ("PAIA"), as amended.

1.2.2 This Manual also supports the Protection of Personal Information Act, 4 of 2013 ("POPIA"), to the extent that records requested may contain personal information.

1.2.3 Access to records may be granted, limited or refused in accordance with PAIA, POPIA, any applicable law, contractual confidentiality obligations and lawful grounds for refusal.

1.3 Availability of this Manual

1.3.1 This Manual must be made available on request and, where applicable, on the Kairos website or through another reasonable public access channel.

1.3.2 A copy may be requested from the Kairos Information Officer using the contact details in section 2.

2. Kairos Details and Information Officer

2.1 Organisation Details

Item	Detail
Registered / Trading Name	Kairos Computer Risk Management
Registration Number	2009/034954/23
Primary Jurisdiction	South Africa
Physical Address	1st Floor, Constantia Emporium, Ladies Mile, Road, Constantia, 7806
Postal Address	1st Floor, Constantia Emporium, Ladies Mile, Road, Constantia, 7806
Website	https://kairoscrm.co.za
Main Contact Email	info@kairoscrm.co.za
Telephone	0215197116

2.2 Information Officer Details

Role	Detail
Information Officer	Gary Grant Adams
Title	CTIO
Email for PAIA / POPIA Requests	informationofficer@kairoscrm.co.za

Telephone	0215197116

2.2.1 The Information Officer is responsible for receiving and coordinating PAIA requests, POPIA-related requests and privacy-related enquiries.

2.2.2 Kairos may appoint a Deputy Information Officer to assist with PAIA and POPIA administration. Deputy Information Officer details must be recorded once formally appointed.

3. Guide on How to Use PAIA

3.1 Information Regulator Guide

3.1.1 The Information Regulator has published a Guide on how to use PAIA. The Guide explains the objectives of PAIA, how to make requests for access to records, assistance available from Information Officers, fees, remedies and related processes.

3.1.2 The Guide may be obtained from the Information Regulator or requested through Kairos' Information Officer where reasonably available.

3.2 Information Regulator Contact Details

Item	Detail
Information Regulator Website	https://inforegulator.org.za
General Email	enquiries@inforegulator.org.za
PAIA Enquiries	PAIAComplaints@inforegulator.org.za
POPIA Enquiries	POPIAComplaints@inforegulator.org.za

4. Records Automatically Available

4.1 Records Available Without a Formal PAIA Request

4.1.1 Certain records may be available without submitting a formal PAIA request, depending on public availability, confidentiality, ownership and security restrictions.

4.1.2 Examples may include publicly available marketing material, company profile information, published policies, website information, service brochures, public contact details and public notices.

4.1.3 Records that contain confidential information, client information, employee information, security information, privileged information or third-party information will not be automatically available.

5. Categories of Records Held by Kairos

5.1 Corporate and Governance Records

5.1.1 Company registration records.

5.1.2 Shareholder or ownership records where applicable.

5.1.3 Governance policies and procedures.

5.1.4 Committee or management records.

5.1.5 Insurance records.

5.1.6 Internal approvals and authorizations.

5.1.7 Risk and compliance records.

5.2 Financial and Accounting Records

5.2.1 Invoices and quotations.

5.2.2 Purchase orders.

5.2.3 Supplier records.

5.2.4 Banking and payment records.

5.2.5 Tax records.

5.2.6 Financial statements and management accounts.

5.2.7 Asset registers.

5.3 Human Resources Records

5.3.1 Employee records.

5.3.2 Contractor records.

5.3.3 Employment contracts.

5.3.4 Training records.

5.3.5 Disciplinary records.

5.3.6 Leave records.

5.3.7 Performance records.

5.3.8 Payroll-related records where applicable.

5.4 Client and Service Records

5.4.1 Client agreements and statements of work.

5.4.2 Support tickets and service desk records.

5.4.3 Project records.

5.4.4 Service reports.

5.4.5 Security assessment records.

5.4.6 Client correspondence.

5.4.7 Technical support documentation.

5.4.8 Client environment information where authorised.

5.5 ICT, Security and Technical Records

5.5.1 System configuration records.

5.5.2 Access control records.

5.5.3 Administrator account records.

5.5.4 Audit logs.

5.5.5 Security incident records.

5.5.6 Backup and restore records.

5.5.7 Change management records.

5.5.8 Network and infrastructure documentation.

5.5.9 Endpoint, cloud, email and security tool records.

5.5.10 Access to ICT, cybersecurity, infrastructure, credential, vulnerability, incident, firewall, backup or security architecture records may be restricted where disclosure could compromise confidentiality, security, safety, client obligations or legal rights.

5.6 POPIA and Privacy Records

5.6.1 Processing activity records.

5.6.2 Data subject request records.

5.6.3 Security incident and data breach records.

5.6.4 Operator and sub-operator records.

5.6.5 Cross-border transfer records.

5.6.6 Privacy impact assessment records.

5.6.7 Retention and disposal records.

5.6.8 Privacy notices and paia-related records.

6. Processing of Personal Information

6.1 Purpose of Processing

6.1.1 Kairos processes personal information for legitimate business purposes, including client service delivery, ICT support, managed services, cybersecurity support, governance consulting, contract administration, billing, supplier management, employee administration, compliance, security monitoring and incident response.

6.2 Categories of Data Subjects

6.2.1 Employees and job applicants.

6.2.2 Clients and client representatives.

6.2.3 Users supported in client environments.

6.2.4 Suppliers and service providers.

6.2.5 Contractors and consultants.

6.2.6 Website visitors and persons making enquiries.

6.2.7 Data subjects whose information is processed in client systems where kairos acts as operator.

6.3 Categories of Personal Information

6.3.1 Names and surnames.

6.3.2 Business contact details.

6.3.3 Identity and account information.

6.3.4 Employment and HR information.

6.3.5 Billing and financial information.

6.3.6 Support ticket information.

6.3.7 Device, endpoint and system information.

6.3.8 Logs, audit records and security events.

6.3.9 Communications and correspondence.

6.3.10 Special personal information only where lawful, necessary and authorised.

6.4 Recipients of Personal Information

6.4.1 Personal information may be shared with authorised employees, contractors, service providers, operators, sub-operators, professional advisors, regulatory authorities, law enforcement bodies, clients or other parties where legally permitted and necessary for the relevant purpose.

6.5 Cross-Border Transfers

6.5.1 Personal information may be stored, accessed or processed outside South Africa where cloud services, email platforms, security tools, backup platforms or other authorised services are used.

6.5.2 Cross-border transfers must be assessed in terms of POPIA, contractual requirements and applicable safeguards. Kairos is formalising a Cross-Border Transfer Register to support client and operator due diligence requirements.

7. Security Safeguards

7.1 General Safeguards

7.1.1 Kairos implements reasonable technical and organisational safeguards to protect records and personal information against unauthorised access, loss, damage, misuse, alteration, disclosure or destruction.

7.1.2 Safeguards may include access control, least privilege, MFA where appropriate, endpoint protection, secure configuration, backups, incident response, physical security, acceptable use controls, confidentiality obligations and third-party controls.

7.2 Related Security Policies

7.2.1 This Manual must be read together with the Kairos POPIA and Data Protection Policy, Information Security Policy, Cybersecurity Policy, Backup and Disaster Recovery Policy, ICT Incident Response Policy, Cybersecurity

Incident Response Plan, User Privilege and Password Management Policy, Acceptable Use Policy, Laptop and Mobile Device Policy, Secure Area Access Policy and Third-Party and Sub-Operator Management Policy.

8. Procedure for Requesting Access to Records

8.1 Submitting a Request

8.1.1 A requester must submit a written request to the Kairos Information Officer using the prescribed PAIA form or another written format accepted by Kairos.

8.1.2 The request must identify the record requested, provide sufficient detail to locate the record, identify the requester, state the right being exercised or protected where required, and provide contact details for communication.

8.2 Proof of Identity and Authority

8.2.1 Kairos may require proof of identity, authority, mandate or representation before processing a request.

8.2.2 Where a request is made on behalf of another person, Kairos may require proof of authorization.

8.3 Processing the Request

8.3.1 Kairos will consider the request in terms of PAIA, POPIA, confidentiality obligations, client obligations and applicable grounds for refusal.

8.3.2 Kairos may request clarification where the request is unclear or insufficiently specific.

8.3.3 Kairos may grant access, grant partial access, refuse access, or transfer/redirect the request where required by law.

9. Grounds for Refusal or Limited Access

9.1 Possible Grounds for Refusal

9.1.1 Access to a record may be refused or limited where PAIA permits or requires refusal.

9.1.2 Grounds may include protection of personal information of another person, confidential information of third parties, commercial information, privileged information, safety or security concerns, law enforcement matters, research information, client confidentiality, contractual restrictions, or records that may compromise ICT or cybersecurity controls.

9.2 Partial Access

9.2.1 Where possible, Kairos may provide partial access to a record after redacting information that may lawfully be withheld.

10. Fees

10.1 Request and Access Fees

10.1.1 Kairos may charge fees as permitted under PAIA and applicable regulations, including request fees, access fees, reproduction fees, search and preparation fees and postage or delivery costs where applicable.

10.1.2 A requester will be advised of applicable fees before access is provided where required.

11. Remedies and Complaints

11.1 Internal Engagement

11.1.1 A requester who is dissatisfied with Kairos' response may contact the Kairos Information Officer to seek clarification or review of the matter.

11.2 Information Regulator

11.2.1 A requester may lodge a complaint with the Information Regulator or seek other remedies available under PAIA where applicable.

12. POPIA and Data Subject Requests

12.1 Data Subject Requests

12.1.1 Requests for access to, correction of, deletion of, or objection to processing of personal information may be managed under POPIA, PAIA or both, depending on the nature of the request.

12.1.2 Where Kairos processes personal information as Operator for a client, Kairos may refer to the client Responsible Party and assist the client according to documented instructions and contractual requirements.

13. Availability, Review and Updates

13.1 Availability

13.1.1 This Manual must be made available in accordance with PAIA requirements and reasonable public access arrangements.

13.2 Review

13.2.1 This Manual must be reviewed at least annually or when there are material legal, business, operational, structural, processing, contact detail or governance changes.

13.2.2 The next scheduled review date is 21 October 2026.

14. Approval

14.1 Approval Statement

14.1.1 This Kairos PAIA Manual was approved by the Kairos CTIO and forms part of the Kairos POPIA and information governance framework.

Approved By	Title	Signature	Date
Gary Grant Adams	CTIO	original signed copy retained internally	17 October 2025

Appendix A. Request Intake Checklist

A.1 Name and contact details of requester.

A.2 Proof of identity or authority where required.

A.3 Description of record requested.

A.4 Right to be exercised or protected where required.

A.5 Preferred form of access.

A.6 Fee confirmation where applicable.