BEE | Training | Skills Development
Anchor Africa
YOUR BUSINESS STABILITY PARTNER

031 764 1311
084 556 2010
sune@anchorafrica.co.za
www.anchorafrica.co.za

PAIA MANUAL

Prepared in terms of Section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

And in accordance with the Protection of Personal Information Act, 2013 (POPIA)

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1 IO: Information Officer
1.2 DIO: Deputy Information Officer
1.3 Minister: Minister of Justice and Correctional Services
1.4 PAIA: Promotion of Access to Information Act No. 2 of 2000 (as Amended)
1.5 POPIA: Protection of Personal Information Act No. 4 of 2013
1.6 Regulator: Information Regulator
1.7 Republic: Republic of South Africa
1.8 BBBEE: Broad-Based Black Economic Empowerment
1.9 EE: Employment Equity
1.10 WSP: Workplace Skills Plan
1.11 CIPC: Companies and Intellectual Property Commission
1.12 SARS: South African Revenue Service
1.13 SETA: Sector Education and Training Authority
1.14 UIF: Unemployment Insurance Fund
1.15 SDL: Skills Development Levy
1.16 ROPA: Records of Processing Activities
1.17 SLA: Service Level Agreement
1.18 CPD: Continuing Professional Development
1.19 MOI: Memorandum of Incorporation
1.20 LMS: Learning Management System

2. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to:

2.1 Check categories of records held which are available without a formal PAIA request.
2.2 Understand how to request access to a record.
2.3 Know the description of records available in terms of other legislation.
2.4 Access contact details of the Information and Deputy Information Officer(s).
2.5 Know how to obtain the PAIA Guide from the Regulator.
2.6 Know the body's personal information processing activities and related safeguards.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION

3.1 Information Officer:
Name: Sune Koegelenberg
Tel: 084 556 2010
Email: sune@anchorafrica.co.za

Note: ***The Deputy Information Officer*** has been designated in terms of Section 17(1) of PAIA and Section 56 of POPIA as the **primary contact person** for all PAIA and POPIA requests and enquiries, ensuring maximum accessibility for requesters. The Deputy Information Officer works in close collaboration with the Information Officer to facilitate all access requests.

3.2 Deputy Information Officer:
Name: Jan Koegelenberg
Tel: 081 024 2805
Email: jandre@anchorafrica.co.za

3.3 General Access Email:
Email: jandre@anchorafrica.co.za

3.4 Head Office:
Physical Address: Unit 3, 10 Doncaster Place, Derby Downs Office Park, Westville, 3629
Tel: 031 764 1311
Email: jandre@anchorafrica.co.za
Website: https://anchorafrica.co.za/

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.
2. The aforesaid Guide contains the description of:
    - the objects of PAIA and POPIA;
    - the postal and street address, phone and fax number and, if available, electronic mail address of the Information Officer of every public body, and every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA;
    - the manner and form of a request for access to a record of a public body contemplated in section 11 and access to a record of a private body contemplated in section 50;
    - the assistance available from the IO of a public body in terms of PAIA and POPIA;
    - the assistance available from the Regulator in terms of PAIA and POPIA;
    - all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging an internal appeal, a complaint to the Regulator, and an application to a court;
    - the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
    - the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;
    - the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and
    - the regulations made in terms of section 92.

3. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.
4. The Guide can also be obtained:
    - upon request to the Information Officer or Deputy Information Officer;
    - from the website of the Regulator (https://inforegulator.org.za/).

5. RECORDS HELD BY THE COMPANY

Anchor Africa (Pty) Ltd maintains various records in both physical and electronic formats to support its operational, financial, legal, and compliance obligations as a training and consulting service provider. These records are securely stored and managed in line with applicable legislation, including the Promotion of Access to Information Act (PAIA), the Protection of Personal Information Act (POPIA), and the Companies Act.

The categories of records held include, but are not limited to, the following:

5.1 Company Records

These are documents that relate to the legal and statutory existence of the company:

- Certificate of Incorporation (CoR 14.3)
- Memorandum of Incorporation (MOI)
- Company registration certificate and amendments
- Shareholder registers and shareholding certificates
- Board resolutions and minutes of directors' meetings
- Company organogram and governance structures
- Statutory returns submitted to the CIPC

5.2 Financial and Accounting Records

These records are maintained for financial management, statutory reporting, tax compliance, and auditing purposes:

- Annual financial statements
- General ledger and journals
- Trial balances and working papers
- Tax returns (VAT, PAYE, UIF, SDL, Income Tax)
- Invoices and receipts
- Bank statements and reconciliations
- Asset registers and depreciation schedules
- Internal and external audit reports

- Budgets and financial forecasts

5.3 Employee and Human Resource Records

These records support employee administration and compliance with labour legislation:

- Employment contracts and job descriptions
- Payroll records and payslips
- Employee leave records (sick, annual, maternity, family responsibility)
- Performance appraisals and disciplinary records
- Training and skills development plans, including WSP submissions
- Equity and diversity statistics
- Health and safety incident records
- Records relating to employee benefits (medical aid, provident fund)
- Employee personal information as regulated under POPIA

5.4 Client and Supplier Records

These are records relating to the company's commercial relationships with training clients and service providers:

- Client databases and contact details
- Training service agreements and contracts
- Training needs assessments and skills audits
- BBBEE consultation agreements and reports
- POPIA compliance project documentation
- Skills development project files
- Client invoices, delivery notes, and correspondence
- Credit applications and account opening forms
- Supplier agreements, service level agreements (SLAs) and contracts
- Procurement documentation (quotations, purchase orders)
- Supplier performance evaluations
- BBBEE certificates and vendor compliance documentation

5.5 Training and Consulting Service Records

These records are specific to Anchor Africa's core business of providing training and consulting services:

- Training course materials and curricula
- Learner registration and attendance records

- Assessment results and certification records
- SETA accreditation documentation
- Training provider registration certificates
- Facilitator qualifications and profiles
- Skills development reports and analytics
- BBBEE verification certificates and scorecards
- BBBEE strategy and implementation plans
- POPIA compliance assessment reports
- Training evaluation and feedback forms

5.6 IT, Network, and Website Logs

These records are generated from company ICT systems for monitoring, cybersecurity, and business continuity purposes:

- Email and network security
- Software licence records
- Backup and recovery logs

5.7 POPIA Compliance and Data Protection Records

These records support the organisation's compliance with the Protection of Personal Information Act:

- Data subject consent forms and privacy notices
- Personal information impact assessments
- Records of processing activities (ROPA)
- Information Officer appointment and training records
- Data breach incident registers and investigation reports
- PAIA and POPIA policies and procedures
- Records of training and awareness sessions conducted

5.8 Online Training Platform Records

These records are generated through the operation of the company's online learning management system and digital training infrastructure:

- User registration and profile information
- Course enrolment and progression records
- Assessment submissions, results, and grading records

- Learning analytics and engagement metrics (time spent, modules completed, login frequency)
- Discussion forum posts and learner-to-learner or learner-to-facilitator communications
- Digital certificates and completion records
- Payment and subscription records (if applicable)
- Platform access logs, including IP addresses, device identifiers, and session data
- Online training platform user terms and conditions
- User-generated content (assignments, portfolios, project submissions)
- Video conferencing recordings (if live sessions are recorded)
- Platform performance and uptime monitoring logs
- Third-party integration logs (e.g., SETA reporting interfaces, payment gateways)
- User feedback, ratings, and course evaluations submitted via the platform

6. AUTOMATICALLY AVAILABLE RECORDS

In accordance with Section 52 of PAIA, the following records are automatically available to the public and may be accessed without the need to formally request them through a PAIA process. These records are freely available on the company website or by request via email:

- Company profile and service brochures
- Website content, including service and training descriptions
- Marketing materials, Newsletters, and course catalogues
- PAIA and POPIA compliance policies and notices
- Privacy Policy
- Terms and Conditions of Service
- Information about the company's structure and locations
- Company contact details and operational hours
- BBBEE Certificate or Affidavit (if voluntarily disclosed)
- Newsletters or press releases
- Public training schedules and course information
- Accreditation certificates and registrations
- PAIA Manual
- Platform privacy policy
- Public course catalogue and descriptions available via the online platform

- Platform technical requirements and system specifications

7. PROCESSING OF PERSONAL INFORMATION

Anchor Africa (Pty) Ltd processes personal information in accordance with the Protection of Personal Information Act, 2013 (POPIA), and takes all reasonable steps to protect the confidentiality, integrity, and availability of such information. Personal information is collected and processed for legitimate, lawful, and business-related purposes as detailed below:

7.1 Purpose of Processing Personal Information

Anchor Africa collects and processes personal information for the following purposes:

Fulfilling Legal and Contractual Obligations:
To comply with applicable South African legislation and to execute agreements with clients, suppliers, employees, contractors, and training participants.

Human Resources and Employment Administration:
For the management of employees, including recruitment, employment contracts, payroll processing, leave administration, performance management, and benefits administration (medical aid, pension/provident fund).

Client and Training Participant Management:
To manage client accounts, training registrations, respond to enquiries, deliver training and consulting services, issue invoices and collect payments, maintain learner records, and conduct skills assessments.

Training and Skills Development Services:
To deliver training programmes, maintain learner records, conduct assessments, issue certificates, report to SETAs, manage WSP submissions, and conduct skills audits.

BBBEE Consulting Services:
To conduct BBBEE assessments, prepare verification reports, develop transformation strategies, and provide ongoing BBBEE consulting support.

POPIA Compliance Services:
To conduct data protection impact assessments, develop POPIA compliance programmes, provide training on data protection, and support clients with regulatory compliance.

Online Training Platform Administration and Service Delivery:
To register users and manage learner accounts on the online training platform; to deliver online training courses, assessments, and certification programmes; to track learner progress, engagement, and competency development; to facilitate communication between learners, facilitators, and support staff; to generate learning analytics for continuous improvement of training content and delivery; to provide technical support and troubleshoot platform issues; to process payments for course enrolments, subscriptions, or certification fees (if applicable); to issue digital certificates and maintain verifiable credential records; to enable integration with third-party systems, including SETA reporting portals and payment gateways; to monitor platform security, prevent unauthorised access, and detect fraudulent activity; to comply with quality assurance requirements under the Skills Development Act and SETA accreditation standards.

Financial and Tax Administration:
To maintain accounting records, perform internal and external audits, prepare tax submissions, and comply with financial reporting requirements.

Regulatory Compliance and Governance:
To comply with obligations under POPIA, PAIA, the Companies Act, Skills Development Act, BBBEE Act, and employment and labour-related legislation.

Marketing and Promotional Communication:
To distribute training information, newsletters, or marketing material to clients or potential clients, where consent has been obtained in accordance with POPIA.

IT and Cybersecurity Management:
To monitor network access, secure systems, and prevent unauthorised access, or misuse of information technology resources.

Health and Safety Obligations:
To record, monitor, and respond to health and safety incidents and ensure compliance with the Occupational Health and Safety Act.

7.2 Description of the Categories of Data Subjects

Anchor Africa processes personal information in relation to the following categories of data subjects:

- Employees (past and present)
- Prospective employees (job applicants)
- Clients and customers (individuals and representatives of juristic persons)
- Training participants and learners
- Suppliers, vendors, and service providers
- Directors, shareholders, and authorised signatories
- Website users and online enquirers
- Online platform users (including registered learners, guest users, and facilitators accessing the platform)

7.3 Categories of Personal Information Processed

The types of personal information processed may include, but are not limited to:

- Full name and contact details (email address, phone number, physical address)
- South African identity number or company registration details
- Employment history, qualifications, and performance records
- Training records, certifications, and competency assessments
- Financial information (bank account details, credit records, tax numbers)
- Correspondence history and transactional data
- System access credentials and usage logs

- Demographic information (e.g., race, gender, disability status – for EE and BBBEE purposes)
- Health and vaccination information (as permitted and required by law)
- Educational qualifications and professional certifications
- Platform username, password (hashed), and authentication credentials
- IP addresses, device identifiers, and browser information
- Learning activity data (courses accessed, time spent, modules completed, assessment attempts)
- User-generated content (forum posts, assignment submissions, comments)
- Payment and billing information (credit card details, billing address – if processed via the platform)
- Geolocation data (where relevant for compliance or service delivery purposes)
- Session logs and platform interaction data
- Digital certificates and credentialing records
- Technical support correspondence and issue resolution records

7.4 Legal Grounds for Processing

Processing is based on one or more of the following lawful grounds in terms of POPIA:

- The data subject's consent
- Fulfilment of a contractual obligation
- Compliance with legal or regulatory requirements
- Protection of a legitimate interest of the data subject
- Pursuit of the company's legitimate interests, provided such interests do not override the rights of the data subject

8. REQUEST PROCEDURES

8.1 How to Make a Request for Access to Records

Any person may request access to records held by Anchor Africa (Pty) Ltd by following the prescribed procedures set out in the Promotion of Access to Information Act, 2000 (PAIA) and its Regulations.

8.2 Submission of Request

Requests for access to records must:

- Be made in writing, using the prescribed PAIA Request Form 2 (Annexure A of the 2021 Regulations).
- Contain all the information required in terms of section 53 of PAIA.

- The prescribed form can be accessed by using the following hyperlink: InfoRegSA-PAIA-Form02-Reg7.pdf.
- The prescribed Form 2 is also available from the Information Regulator's website: www.inforegulator.org.za

8.3 Where to Submit Requests

Requests must be submitted to:

Deputy Information Officer: Jan Koegelenberg
Email: jandre@anchorafrica.co.za
Telephone: 081 024 2805

Alternatively

Information Officer: Sune Koegelenberg
Email: sune@anchorafrica.co.za
Telephone: 084 556 2010

Physical Address: Unit 3, 10 Doncaster Place, Derby Downs Office Park, Westville, 3629.
Telephone: 031 764 1311

8.4 Information Required in Request

A request for access to a record must contain the following information:

- Full name and contact details of the requester
- The right the requester is seeking to exercise or protect, and an explanation of why the record is required for the exercise or protection of that right
- Sufficient detail to enable the Information Officer to identify the type record(s) requested
- The preferred form of access to the record (inspection, copy, transcript, etc.)
- The postal address or email address of the requester
- If the requester wishes to be informed by telephone or email of the decision, the telephone number and/or email address
- If the request is made on behalf of another person, proof of the capacity in which the requester is making the request

8.5 Response Timeframes

8.5.1 Initial Response

The Information Officer must, within 30 days of receipt of the request:

- Decide whether to grant or refuse the request; and
- Give notice of the decision to the requester

8.5.2 Extension of Time

The 30-day period may be extended for a further period of not more than 30 days if:

- The request is for a large number of records or requires a search through a large number of records
- Consultation with third parties is necessary
- Additional time is needed to determine whether any provision of Chapter 4 of PAIA applies

8.5.3 Notice of Extension

If the time period is extended, the requester must be notified in writing within the original 30-day period, stating:

- The extended period and reasons for the extension
- That the requester may lodge a complaint with the Information Regulator or apply to court

8.6 Third Party Consultation

If the requested record contains information about a third party, the Information Officer may need to:

- Give notice to the third party of the request
- Allow the third party to make representations regarding disclosure
- Consider any representations before making a decision

9. PRESCRIBED FEES

9.1 Fee Structure

The following fees are payable for requests made in terms of PAIA, as prescribed in Government Notice R. 187 of 15 February 2002 (as amended):

9.2 Request Fee

A request fee of R140.00 is payable by every requester except:

- Personal requesters seeking access to records containing their own personal information
- Requests in the public interest

9.3 Access Fees

Service	Fee
For every photocopy of an A4-size page or part thereof	R2.00
For every printed copy of an A4-size page or part thereof held on a computer or in electronic/machine-readable form	R2.00
For a copy in a computer-readable form on a compact disc	R70.00

Service	Fee
For a transcription of visual images for an A4-size page or part thereof	R40.00
For a copy of the visual images	R60.00
For a transcription of an audio record for an A4-size page or part thereof	R20.00
For a copy of an audio record	R70.00

9.4 Postal Fees

Actual postal fees for delivery will be charged where applicable.

9.5 Search and Preparation Fees

For searches conducted by or on behalf of Anchor Africa: R145.00 for each hour or part of an hour reasonably required for the search and preparation of the record for disclosure. This fee is only applicable to requests other than personal requests.

9.6 Payment Requirements

9.6.1 Request Fee Payment

- The request fee must be paid before the request will be processed
- Proof of payment must be provided
- If the request fee is not paid within 30 days, the request will be regarded as withdrawn

9.6.2 Access Fee Payment

- The access fee must be paid before access to the record is granted
- An estimate of access fees may be provided and a deposit required
- If the access fee is not paid within 30 days of notification, access to the record will be refused

9.7 Fee Exemptions

No request fee is payable where:

- The requester is seeking access to a record containing that requester's personal information
- The Information Officer is satisfied that the request is made in the public interest

10. APPEALS AND COMPLAINTS

10.1 Internal Appeals

Anchor Africa (Pty) Ltd does not have an internal appeal mechanism as it is not required for private bodies under PAIA. Requesters who are dissatisfied with a decision may proceed directly to lodge a complaint with the Information Regulator or approach a court.

10.2 Complaints to the Information Regulator

10.2.1 Right to Complain

If you are dissatisfied with the response to your PAIA request, you may lodge a complaint with the Information Regulator within 30 days of:

- The decision being communicated to you; or
- The expiry of the response period without receiving a response

10.2.2 Information Regulator Contact Details

Physical Address: Woodmead North Office Park, 54 Maxwell Dr, Woodmead, Johannesburg, 2191
Postal Address: P.O. Box 31533, Braamfontein, Johannesburg, 2017
Email: complaints.IR@justice.gov.za or enquiries@inforegulator.org.za
Telephone: 010 023 5200
Website: https://inforegulator.org.za/

10.2.3 Complaint Requirements

Your complaint should include:

- Your contact details
- Details of the PAIA request made
- The response received (or lack thereof)
- The reasons why you believe the response was inadequate
- Copies of relevant correspondence

10.3 Court Applications

10.3.1 Right to Approach Court

You may apply to court for appropriate relief if you are not satisfied with:

- A decision of the Information Officer
- A decision by the Information Regulator
- The failure of the Information Officer to respond within the prescribed timeframes

10.3.2 Time Limits

Applications to court must generally be made within 30 days of the relevant decision or event.

10.3.3 Legal Representation

You may wish to seek legal advice before approaching the court, as legal costs may be awarded against an unsuccessful party.

11. DATA SUBJECT CATEGORIES AND INFORMATION

Anchor Africa (Pty) Ltd processes personal information relating to multiple categories of data subjects in the course of conducting its training and consulting business operations. The types of

personal information collected are appropriate to the nature and purpose of the relationship with each data subject.

Category of Data Subjects	Types of Personal Information Processed
Employees (current and former)	Full name, ID number, contact details, residential address, date of birth, employment contract details, remuneration and benefits, job title and responsibilities, leave records, disciplinary records, performance evaluations, medical aid and pension fund information, next-of-kin details, employment equity data (race, gender, disability status)
Prospective Employees	Curriculum Vitae (CV), qualifications, references, identity number, contact details, interview notes, employment screening results (e.g., criminal record, credit checks – if applicable)
Clients and Customers	Full name or registered business name, contact person details, contact information (email, phone, physical address), billing information, VAT number, service agreements, correspondence, project documentation
Training Participants and Learners	Full name, ID number, contact details, educational background, training records, assessment results, certification details, attendance records, skills development plans
Suppliers, Vendors, and Service Providers	Company registration information, BBBEE certificate, VAT number, contact persons, service agreements, business addresses, payment and banking details, pricing and quotation history
Website Visitors and Online Users	IP addresses, browser type, geographic location, device information, pages visited, interaction timestamps, cookies and usage logs (subject to cookie consent policy)
Directors, Shareholders, and Key Individuals	Name, ID number, shareholding structure, directorships, personal contact details (where relevant), and declarations of interest for compliance or governance purposes
Visitors to Company Premises	Full name, contact number, vehicle registration, date and time of visit, person visited, and CCTV footage (if applicable)
Online Platform Users (Learners and Facilitators)	Full name, email address, contact number, username, password (hashed), ID number (if required for certification), profile information, course enrolment records, learning progress and completion data, assessment results, assignment submissions, forum posts and communications, IP addresses, device information, session logs, payment and billing information (if applicable), digital certificates and credentials, technical support queries and correspondence

All personal information collected is limited to what is necessary, relevant, and proportionate to the purpose for which it is collected. Such information is processed in accordance with POPIA's eight

conditions for lawful processing, and retained only as long as necessary for operational, legal, or regulatory purposes.

12. RECIPIENTS OF PERSONAL INFORMATION

Anchor Africa (Pty) Ltd shares personal information with authorised third parties only when such disclosure is necessary for the fulfilment of legitimate business, legal, or contractual purposes, or where required by law. All third-party recipients are contractually obligated to maintain the confidentiality and integrity of personal information in accordance with POPIA.

The following categories of recipients may receive personal information, as relevant to the purpose of processing:

Category of Personal Information	Recipients or Categories of Recipients
Identity numbers, names, job-related data	Government and Regulatory Bodies, including SARS, the Department of Labour, SETAs, and the Companies and Intellectual Property Commission (CIPC) – for statutory reporting and compliance
Employment information, earnings, leave, tax data	Payroll service providers, benefit administrators, and statutory funds (e.g., UIF, Compensation Fund) – for HR administration
Training records, learner information	SETAs, Training Quality Assurers, and Certification Bodies – for skills development reporting, learnership tracking, and certification
Contact details, contract details, legal agreements	Legal and Compliance Advisors – for legal representation, auditing, dispute resolution, and POPIA/PAIA compliance
Company registration details, contact information, financial transactions	Service Providers and Subcontractors, such as IT consultants, software vendors, courier services, and maintenance contractors – in fulfilment of contractual services
Payment and financial details	Banks and Financial Institutions – for transaction processing, account verification, and collections
Technical and device usage information	Cybersecurity and IT Infrastructure Providers – for system protection, monitoring, and incident response
Medical and emergency information	Health and Safety Officers, Emergency Responders, or medical practitioners – where required for compliance or emergency response
Platform login credentials, learner activity data, assessment results	Online Learning Management System (LMS) Provider – for platform hosting, maintenance, and technical support

Category of Personal Information	Recipients or Categories of Recipients
Payment and billing information	Payment Gateway Providers and Financial Institutions – for processing course fees, subscriptions, and certification payments (if applicable)
IP addresses, device data, session logs	Cloud Hosting and Infrastructure Providers – for secure data storage, server management, and platform availability
Learner registration and completion records	SETAs and Quality Assurance Bodies – for reporting, verification, and compliance with Skills Development Act requirements (where applicable)
Technical support queries and system logs	IT Support and Cybersecurity Service Providers – for troubleshooting, system monitoring, and security incident response

Where personal information is shared with third-party service providers in relation to the online training platform, Anchor Africa (Pty) Ltd ensures that such providers are contractually bound as operators in terms of Section 1 of POPIA.

13. SECURITY SAFEGUARDS

General Description of Information Security Measures

Anchor Africa (Pty) Ltd implements a comprehensive set of technical, physical and administrative security measures to protect personal information from loss, unauthorised access, interference, modification, destruction, or disclosure. These safeguards are aligned with the requirements of the Protection of Personal Information Act (POPIA) and are reviewed regularly for effectiveness.

The following security measures are in place:

Physical Security:

- Secure office premises with controlled access
- Locked filing cabinets and storage areas for physical documents
- Visitor access control

Technical Security:

- Endpoint protection on all devices with antivirus
- Regular software updates
- Secure backup systems
- Access controls based on the principle of least privilege
- Secure password policies
- Data segregation and access controls to prevent unauthorised access to learner records

Administrative Security:

- Information security policies and procedures
- Staff training on data protection
- Background checks for employees handling sensitive information
- Confidentiality agreements with all staff and contractors
- Regular review and updating of security measures
- Incident response procedures and breach notification protocols
- Data retention and disposal policies
- Regular compliance audits and assessments
- Platform user agreements and acceptable use policies
- Privacy notices specific to online platform usage, prominently displayed during registration
- Regular review of third-party operator agreements and data processing arrangements
- Training for staff and facilitators on secure platform usage and data handling practices

Access Controls:

- Role-based access controls
- User authentication and authorization procedures
- Regular review and updating of access rights
- Monitoring and logging of system access

Data Protection Measures:

- Encryption of sensitive data
- Regular data backups with secure storage
- Secure data disposal procedures

Incident Response:

- Documented incident response procedures
- Breach notification procedures in compliance with POPIA
- Recovery and business continuity procedures
- Incident response procedures specific to online platform security breaches, including notification to the LMS provider and affected users

These measures ensure that Anchor Africa (Pty) Ltd maintains the confidentiality, integrity, and availability of personal information in line with POPIA obligations and industry best practice.

14. AVAILABILITY OF THE MANUAL

A copy of this Manual is available:

- At https://anchorafrica.co.za/
- Head office of Anchor Africa (Pty) Ltd for public inspection during normal business hours
- To any person upon request, prescribed PAIA Request Form 2 (Annexure A of the 2021 Regulations), and upon the payment of a reasonable prescribed fee
- To the Information Regulator upon request

15. GROUNDS FOR REFUSAL

Anchor Africa (Pty) Ltd recognises the constitutional right of access to information under Section 32 of the Constitution and supports transparency and accountability. However, access to certain records may be refused in accordance with Chapter 4 of PAIA, particularly where disclosure would result in harm to the rights or interests of the company, third parties, or public safety.

Requests for access to information may be refused on one or more of the following legal grounds:

15.1 Protection of Third-Party Commercial or Confidential Information

Access may be refused if the record contains:

- Trade secrets of a third party
- Financial, commercial, scientific, or technical information, the disclosure of which would likely cause harm to the commercial or financial interests of that third party
- Information supplied in confidence by a third party, the disclosure of which could reasonably be expected to prejudice the third party in negotiations or commercial competition

15.2 Protection of Personal Information of Third Parties

A request may be refused if the record contains personal information about a third party, unless:

- The third party has consented to the disclosure
- The information is publicly available
- The disclosure is in the public interest and outweighs the harm that may result from such disclosure

15.3 Legal Privilege

Records that are subject to legal professional privilege may not be disclosed. This includes:

- Correspondence between the company and its legal advisors
- Documents prepared in anticipation of legal proceedings

15.4 Protection of the Safety of Individuals and the Security of Property

A request may be refused if granting access would:

- Endanger the life or physical safety of any individual

- Prejudice or impair the security of a building, structure, computer system, communication network, or any means of transport

15.5 Protection of the Company's Commercial Activities

Access may be refused if it contains:

- Trade secrets or other commercially sensitive information belonging to the company
- Information that would place the company at a disadvantage in commercial negotiations or competition
- Proprietary training materials, curricula, and methodologies
- Client-specific consulting reports and strategies
- Proprietary online training platform configurations, customisations, and technical architecture that could compromise competitive advantage or platform security if disclosed

15.6 Protection of Research Information

If disclosure would significantly disadvantage the company or a third party in relation to ongoing or future research, access may be refused.

15.7 Manifestly Frivolous or Vexatious Requests

Access may be refused if a request is manifestly frivolous, vexatious, or places an unreasonable administrative burden on the company. Examples of frivolous or vexatious requests include:

- Repetitive requests for the same information without new justification or changed circumstances
- Requests that are clearly intended to harass, intimidate, or disrupt the operations of the company
- Requests that lack any apparent legitimate purpose or connection to the exercise or protection of a right
- Requests for an excessive volume of records that are manifestly beyond the scope of reasonable access
- Requests formulated in deliberately vague or overly broad terms designed to impose administrative burden

All refusals will be provided in writing with reasons, and the requester will be informed of their right to lodge a complaint with the Information Regulator or approach a court for relief in terms of Section 78 of PAIA.

16. ONLINE TRAINING PLATFORM AND POPIA COMPLIANCE

Anchor Africa (Pty) Ltd operates an online training platform to deliver skills development, BBBEE, and compliance training services. The platform collects and processes personal information necessary for user registration, course delivery, assessment, certification, and ongoing learner support.

16.1 Data Subject Rights

Platform users have the right to:

- Access their personal information held on the platform (POPIA Section 23)
- Request correction of inaccurate or outdated information (POPIA Section 24)
- Request deletion of their account and associated data, subject to legal retention requirements (POPIA Section 15)
- Object to certain types of processing, including direct marketing communications (POPIA Section 11(3))
- Withdraw consent for processing activities that are based on consent (POPIA Section 11(2))

Requests to exercise these rights may be submitted to the Deputy Information Officer at jandre@anchorafrica.co.za or the Information Officer at sune@anchorafrica.co.za

16.2 Retention of Platform Data

Personal information collected via the online training platform is retained in accordance with the following principles:

- Learner records required for SETA reporting and certification are retained for a minimum of five years following course completion, in line with Skills Development Act requirements
- Assessment records and credentials are retained to enable verification of qualifications and competencies
- Platform access logs and technical data are retained for cybersecurity and troubleshooting purposes, typically for 12 months unless required for longer periods due to security rinvestigations or legal obligations
- User-generated content (e.g., forum posts, assignment submissions) is retained for the duration of the user's active account and may be anonymised or deleted upon account closure, subject to legal and operational requirements

16.3 Third-Party Service Providers

The online training platform is hosted and supported by third-party service providers who act as operators under POPIA. These providers are contractually obligated to process personal information only on Anchor Africa's instruction and to implement appropriate security measures. Users acknowledge and consent to the involvement of these operators when registering on the platform.

16.4 Data Breaches and Incident Notification

In the event of a data breach affecting the online training platform, Anchor Africa will:

- Investigate the breach and assess the risk of harm to affected data subjects
- Notify the Information Regulator as soon as reasonably possible, and within 72 hours where the breach is likely to cause harm (POPIA Section 22)
- Notify affected platform users directly, providing information on the nature of the breach, potential consequences, and remedial measures taken
- Implement corrective actions to prevent recurrence and mitigate harm

17. REVIEW AND UPDATES

Compiled on: 6 August 2025 (Version 1.0)
Updated on: 3 October 2025 (Version 1.1)
Next review: 6 August 2026

_____

Issued by:

Sune Koegelenberg
Director - Anchor Africa (Pty) Ltd

END OF MANUAL