PAIA MANUAL

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

DATE OF COMPILATION: 10/10/2025

DATE OF REVISION: 01/10/2026

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1 "CEO" Chief Executive Officer

1.2 "DIO" Deputy Information Officer;

1.3 "IO" Information Officer;

1.4 "Minister" Minister of Justice and Correctional Services;

1.5 "PAIA" *Promotion of Access to Information Act No. 2 of 2000*(as

Amended;

1.6 "POPIA" *Protection of Personal Information Act No.4 of 2013*;

1.7 "Regulator" Information Regulator; and

1.8 "Republic" Republic of South Africa

2. PURPOSE OF PAIA MANUAL

2.1   This PAIA Manual is useful for the public to check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

2.2   have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

2.3   know the description of the records of the body which are available in accordance with any other legislation;

2.4   access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

2.5   know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

2.6   know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

2.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;

2.8 know the recipients or categories of recipients to whom the personal information may be supplied;

2.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

2.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF AFRIFORUM (NPO)

3.1. Chief Information Officer
Name: KRIEL, CARL MARTIN
Tel: 0861020030
Email: kallie@afriforum.co.za

3.2. Deputy Information Officer
Name: KAMFER, JACOBUS MARTHINUS
Tel: 0861020030
Email: marnus.kamfer@afriforum.co.za

3.3 Access to information general contacts
Email: help@afriforum.co.za

3.4 National or Head Office
Postal Address: P.O. Box 17216
LYTTELTON

0140

Physical Address: 58 Union Avenue

Kloofsig

Centurion

0157

Telephone: 0861020030

Email: help@afriforum.co.za

Website: https://afriforum.co.za/

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

4.1. 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.

4.2. The Guide is available in each of the official languages and in braille.

4.3. The aforesaid Guide contains the description of-

4.3.1. the objects of PAIA and POPIA;

4.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of:

4.3.2.1. the Information Officer of every public body, and

4.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA[1] and section 56 of POPIA[2];

---

[1]Section 17(1) of PAIA- For the purposes of PAIA, each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as deputy information officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.

[2]Section 56(a) of POPIA- Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of

4.3.3.   the manner and form of a request for:

    4.3.3.1. access to a record of a public body contemplated in section

          11[3]; and

    4.3.3.2. access to a record of a private body contemplated in section

          50[4];

4.3.4.   the assistance available from the IO of a public body in terms of PAIA and
POPIA;

4.3.5.   the assistance available from the Regulator in terms of PAIA and POPIA;

4.3.6.   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:

    4.3.6.1. an internal appeal;

    4.3.6.2. a complaint to the Regulator; and

    4.3.6.3. an application with a court against a decision by the information

        officer of a public body, a decision on internal appeal or a decision by

        the Regulator or a decision of the head of a private body;

4.3.7.   the provisions of sections 14[5] and 51[6] requiring a public body and private

    body, respectively, to compile a manual, and how to obtain access to a

---

such a number of persons, if any, as deputy information officers as is necessary to perform the duties and
responsibilities as set out in section 55(1) of POPIA

[3] Section 11(1) of PAIA- A requester must be given access to a record of a public body if that requester
complies with all the procedural requirements in PAIA relating to a request for access to that record; and access
to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

[4] Section 50(1) of PAIA- A requester must be given access to any record of a private body if
a) that record is required for the exercise or protection of any rights;
b) that person complies with the procedural requirements in PAIA relating to a request for access to that record;
and
c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

[5] Section 14(1) of PAIA- The information officer of a public body must, in at least three official languages,
make available a manual containing information listed in paragraph 4 above.

[6] Section 51(1) of PAIA- The head of a private body must make available a manual containing the description of
the information listed in paragraph 4 above.

manual;

4.3.8. the provisions of sections 15[7] and 52[8] providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.3.9. the notices issued in terms of sections 22[9] and 54[10] regarding fees to be paid in relation to requests for access; and

4.3.10. the regulations made in terms of section 92[11]

4.4. 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.

4.5. The Guide can also be obtained:

4.5.1. upon request to the Information Officer;

4.5.2. from the website of the Regulator (https://www.justice.gov.za/inforeg/).

4.6 A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours:

4.6.1 (Afrikaans and English)

---

[7] Section 15(1) of PAIA- The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access.

[8] Section 52(1) of PAIA- The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access.

[9] Section 22(1) of PAIA- The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

[10] Section 54(1) of PAIA- The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

[11] Section 92(1) of PAIA provides that –"The Minister may, by notice in the Gazette, make regulations regarding-
(a) any matter which is required or permitted by this Act to be prescribed;
(b) any matter relating to the fees contemplated in sections 22 and 54;
(c) any notice required by this Act;
(d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to
be made available in terms of section 15; and
(e) any administrative or procedural matter necessary to give effect to the provisions of this Act."

5. CATEGORIES OF RECORDS OF AFRIFORUM (NPO) WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS:

5.1. Policy, Legal, and Regulatory Information

    5.2.1   PAIA Manual (required by s 51 PAIA)

    5.2.2   POPIA Privacy Notice / Data Protection Policy

    5.2.3   Cookie and website usage policy

Available on: Footer links and "Legal and Compliance" pages.

5.2. Public Relations and Media Material

    5.2.1   Press releases and media statements

    5.2.2   Official public responses and commentaries

    5.2.3   Newsletters and digital publications (e.g., AfriForum Nuus, AfriForumTV videos)

    5.2.4   Public awareness campaigns (e.g., community safety, environmental, or language rights projects)

Available on: "News", "AfriForumTV", and AfriForum social-media platforms.

5.3. Programmes and Project Information

5.3.1 Descriptions of ongoing campaigns and community projects (Safety, Environment, Education, Local Government, etc.)

5.3.2 Event schedules, training programmes, and workshops open to the public

5.3.3 Volunteer recruitment information and community structures

5.3.4 Public results or outcomes of campaigns (e.g., restored water points, legal victories, safety initiatives)

Available on: Main navigation pages under "Projects", "Get Involved", and "Branches".

5.4. Membership and Public Participation

5.4.1 Membership registration form and process

5.4.2 Membership categories and benefits

5.4.3 Branch contact details and leadership lists (where publicly displayed)

5.4.4 Volunteer opportunities and safety network information

Available on: "Join Us" or "Word lid" pages.

5.5. Financial Transparency and Fundraising

5.5.1 Annual Financial Statements (summaries) or financial highlights (where published)

5.6 . Educational and Informational Material

    5.6.1   Guides and pamphlets on constitutional rights, self-defence, municipal complaints, etc.

    5.6.2   Research reports and position papers authored or commissioned by AfriForum

    5.6.3   Legal information leaflets for community use

Available on: "Resources" or "Downloads" pages.

5.7. Contact and Access Channels

    5.8.1   Office addresses and contact numbers

    5.8.2   Designated Information Officer and Deputy Information Officer contact details

    5.8.3   Online enquiry forms and feedback mechanisms

Available on: "Contact Us" page and footer links.

6. DESCRIPTION OF THE RECORDS OF AFRIFORUM (NPO) WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

No	Legislation	Description of record	Availability
1	Companies Act 71 of 2008	Incorporation & director records	CIPC public register
2	NPO Act 71 of 1997	NPO registration & annual reports	NPO Directorate

3	Income Tax Act 58 of 1962	PBO / tax exemption certificate	SARS
4	BCEA, LRA, COIDA, UIA	Labour and safety registrations	Dept of Labour
5	PSIRA Act / CPA 51 of 1977	Community safety partnerships	PSIRA / SAPS
6	B-BBEE Act 53 of 2003	B-BBEE affidavit	B-BBEE Commission
7	POPIA 4 of 2013	Privacy Notice & IO registration	AfriForum website / Info Regulator
8	PAJA 3 of 2000	Administrative procedures	Internal / On request
9	ECT Act 25 of 2002	Website and digital transparency	Online
10	Archives Act 43 of 1996	Records retention schedules	Internal / On request

7. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY AFRIFORUM (NPO)

7.1. ORGANISATIONAL ADMINISTRATION AND GOVERNANCE

7.1.1   Categories of records:

- Founding documents (MOI, NPO registration certificate, CIPC incorporation records)

- Constitution and governance framework

- Records of directors, and management committees

- Board meeting agendas, minutes, and resolutions

- Delegation of authority registers

- Policies, codes of ethics, and conduct manuals

- Annual reports, strategic plans, and performance reviews

- Decision registers

7.2 MEMBERSHIP AND BRANCH STRUCTURES

7.2.1   Categories of records:

- Membership application forms and databases

- Membership categories, subscription records, and payment histories

- Branch and neigbourhoodwatch establishment and registration records

- Records of branch committee members

- Communication between head office and branches

- Volunteer and community network lists

- Memorandum of understanding documentation with other roleplayers.

7.3. HUMAN RESOURCES AND EMPLOYMENT MATTERS

7.3.1 Categories of records:

- Employee personal and employment records

- Employment contracts and job descriptions

- Leave, performance appraisal, and training records

- Payroll and remuneration documentation

- UIF, PAYE, and compensation fund records

- Disciplinary and grievance procedures

- Recruitment and selection records

7.4. FINANCIAL MANAGEMENT AND FUNDRAISING

7.4.1 Categories of records:

- Annual financial statements and management accounts

- Budgets and expenditure reports

- Donor and sponsor records (subject to POPIA compliance)

- Tax, VAT, and PBO documentation (SARS correspondence)

- Fundraising campaign records and related communications

- Audit reports and accounting records

- Procurement and payment records

7.5. LEGAL, COMPLIANCE, AND POLICY MATTERS

7.5.1 Categories of records:

- PAIA Manual and POPIA compliance documentation

- Correspondence with the Information Regulator

- Legal opinions and compliance reviews

- Litigation and case files (court documents, pleadings, judgments)

- Contracts, agreements, and memoranda of understanding (MOUs)

- Insurance policies and risk management documents

- Statutory registrations and licences

- Last will and testaments (membership benefit)

7.6. PUBLIC RELATIONS, MEDIA, AND COMMUNICATIONS

7.6.1 Categories of records:

- Press releases, public statements, and media briefings

- Newsletters, publications, and reports to members

- Marketing and awareness campaign materials

- Photography, video, and graphic design records

- Website and social media content archives

- Correspondence with journalists and media outlets

- Event and conference materials

7.7. COMMUNITY SAFETY AND SECURITY PROJECTS

7.7.1   Categories of records:

- Project proposals, reports, and operational plans

- Partnership agreements with community safety structures (e.g., GPFs, SAPS, PSIRA-registered partners)

- Incident reports, training records, and patrol data (where applicable)

- Volunteer indemnity forms, code of conduct documents and consent records

- Drone and surveillance project documentation

- Communication logs and safety campaign materials

7.8. ENVIRONMENTAL, AGRICULTURAL, AND COMMUNITY DEVELOPMENT INITIATIVES

7.8.1 Categories of records:

- Project concept documents and implementation reports

- Agreements with partner entities, schools, and sponsors (e.g., Meadow Feeds, National Chicks, etc.)

- Community feedback and beneficiary reports

- Monitoring and evaluation data

- Financial and logistical records for community projects

7.9. EDUCATION, TRAINING, AND ENTERPRISE DEVELOPMENT

7.9.1 Categories of records:

- Training programme content, course outlines, and lesson plans

- Accreditation records (if applicable)

- Student or participant registration lists

- Attendance registers and certificates issued

- Partnership agreements with educational institutions

- Feedback and impact assessments

7.10. INFORMATION TECHNOLOGY AND DIGITAL OPERATIONS

7.10.1 Categories of records:

- Website hosting, maintenance, and analytics records

- Software licences and vendor agreements

- IT infrastructure inventories

- Data protection and cybersecurity policies

- Email and network access control records

- Backup and disaster recovery logs

7.11. MEMBERSHIP SERVICES AND PUBLIC ENQUIRIES

7.11.1 Categories of records:

- General correspondence and enquiry logs

- Complaint records and resolutions

- Helpdesk and call-centre interactions

- Feedback and satisfaction surveys

7.12. PROPERTY AND ASSETS

7.12.1 Categories of records:

- Asset registers and inventories

- Lease agreements (offices, storage, and vehicles)

- Vehicle records and usage logs

- Equipment maintenance schedules

- Insurance and valuation records

7.13. RESEARCH, POLICY, AND ADVOCACY

7.13.1 Categories of records:

- Research reports, position papers, and submissions

- Legal and policy briefs

- Public consultation inputs and advocacy materials

- Correspondence with public bodies and stakeholders

- Copies of parliamentary submissions and media briefings

7.14. HEALTH, SAFETY, AND ENVIRONMENTAL (HSE) COMPLIANCE

7.14.1 Categories of records:

- Occupational health and safety policy and incident records

- Risk assessments and emergency procedures

- Health and safety training records

- Safety audit and compliance reports

7.15. DONOR, STAKEHOLDER, AND AFFILIATE RELATIONS

7.15.1 Categories of records:

- Correspondence with donors, sponsors, and affiliates

- Partnership and collaboration agreements

- Event sponsorship records

- Reports to donors and accountability documentation

Access to the above records will be provided in accordance with PAIA and subject to applicable limitations relating to:

- Protection of personal information (POPIA),

- Confidentiality undertakings,

- Commercial sensitivity, and

- Security of operations and assets.

8. PROCESSING OF PERSONAL INFORMATION

8.1 Purpose of Processing Personal Information

- AfriForum NPC processes personal information primarily to fulfil its organisational objectives as a civil rights and community-based non-profit organisation.

- Personal information is processed in order to:

  o Administer membership and branch structures – maintain member databases, process applications, renewals, and communicate membership benefits.

  o Facilitate community projects and volunteer activities – record volunteer details for safety, environmental, educational, and humanitarian programmes.

  o Conduct advocacy, awareness, and communication – distribute newsletters, campaign updates, and public notices; manage social-media and media relations.

- o Comply with legal and statutory obligations – including reporting to the Information Regulator, CIPC, the Department of Social Development (NPO Directorate), SARS, and labour authorities.

- o Recruit and manage employees and contractors – administer human-resources, payroll, benefits, training, and performance evaluation.

- o Administer financial and donor relations – issue receipts, manage donations, sponsorships, and financial reporting in terms of tax and NPO legislation.

- o Manage litigation, legal assistance, and community complaints – handle information required for internal legal matters, representation, or complaints to authorities.

- o Ensure security, safety, and operational integrity – record CCTV, access-control data, and communication logs for safety projects and office premises.

- o Conduct research and statistical analysis – analyse member demographics and project impact for internal planning and public-interest reporting.

- o Operate digital platforms and online services – manage website registrations, online forms, and electronic communications in accordance with the Electronic Communications and Transactions Act.

8.2 Description of the categories of Data Subjects and of the information or categories of information relating thereto:

- AfriForum NPC processes personal information relating to the following categories of data subjects, and in respect of each, the corresponding categories of personal information:

Category of data subject Processed	Categories / Nature of Personal Information

Members and Supporters	Full name, ID number, contact details, membership number, branch affiliation, payment details, communication preferences, demographic data voluntarily supplied.
Volunteers and Project Participants	Identification and contact details, emergency contact, skills and training records, signed indemnities, participation logs, photographs or video (for awareness/public reporting).
Employees and Job Applicants	Personal details, CVs, qualifications, employment history, remuneration, tax and banking information, disciplinary and performance records, leave and training data.
Donors and Sponsors	Names or company details, contact information, donation or sponsorship amount, correspondence, and financial or tax receipt records (subject to confidentiality).
Beneficiaries and Community Participants	Names and contact details (where relevant), project participation data, correspondence and consent records, demographic or geographic identifiers.
Legal and Administrative Counterparties	Names, identity or registration numbers, correspondence, contract documentation, and related case-file information.
Website Visitors and Online Users	IP address, browser data, online identifiers, cookies, submitted forms, enquiry information, and communication preferences in line with AfriForum's Cookie and Privacy Policy
Suppliers, Service Providers and Consultants	Business registration details, tax/VAT numbers, bank information, contact persons, correspondence, and service agreements.
Stakeholders and Government Officials	Names, positions, contact details, and correspondence relating to partnerships, regulatory engagements, or submissions.
Security and Safety Participants	Names, contact details, patrol logs, incident reports, CCTV images, and equipment allocation data, processed solely for community safety coordination.

All processing is performed lawfully and in accordance with the eight conditions for the lawful processing of personal information as set out in Chapter 3 of the *Protection of Personal Information Act 4 of 2013 (POPIA)*.

Personal information is retained only for as long as necessary to achieve the purpose of processing or as required by law.

Where processing involves special personal information (e.g., biometric data, health status, or political opinions), such processing occurs only under lawful grounds permitted by POPIA and with the data subject's explicit consent.

8.3 The recipients or categories of recipients to whom the personal information

may be supplied:

AfriForum NPC supplies or may supply personal information to the following persons or categories of persons, only to the extent necessary to achieve the lawful purpose for which the information was obtained and subject to appropriate confidentiality and data-protection safeguards:

Category of Personal Information	Recipient or Category of Recipient	Purpose / Lawful Basis of Disclosure
Member and Supporter information (name, contact details, membership number, branch affiliation, communication preferences)	AfriForum regional and branch committees and internal administrative staff	To administer membership, communication, and branch operations
Payment and financial data (banking details, receipts, donor records)	Authorised finance staff, SARS and registered auditors , Financial institutions or payment processors	For accounting, auditing, and statutory tax reporting
Employee and contractor records (HR, payroll, training)	Department of Labour, SARS, Medical aid and pension administrators. External HR/payroll service providers	For statutory compliance, remuneration, and benefits administration
Volunteer and community-safety participant details (contact information, patrol logs, training records)	Registered Community Safety Structures, SAPS Service or Community Police Forums, Insurers or legal counsel (if required)	For coordination of safety operations and legal compliance

Donor and sponsor details (name, contact, donation record)	Finance department, External auditors, Regulatory authorities (if required by law)	For financial management, donor reporting, and statutory disclosure
Beneficiary and project participant data (contact details, participation data)	Partner organisations, schools, or sponsors participating in specific projects	For implementation and monitoring of community or educational projects
Legal and compliance correspondence (case files, contracts, opinions)	External legal advisors and attorneys, Courts and tribunals, Regulators or public authorities	For litigation, compliance, or enforcement purposes
Website and online user data (cookies, analytics, enquiry forms)	IT service providers, Web-hosting and analytics partners, Cyber-security vendors	For site administration, analytics, and security maintenance
Supplier and service-provider information (business contact details, registration and bank info)	AfriForum finance and procurement units, Auditors ,Regulatory agencies	For procurement, payments, and compliance verification
Photographs, video, and media content	Public media outlets, AfriForumTV, Social-media platforms	For awareness, publicity, and campaign communication (only with consent)
Information required by law or regulation	Information Regulator, CIPC, Department of Social Development, SARS, Any other competent authority	To comply with statutory reporting and lawful requests

Personal information is disclosed only where a lawful basis exists under POPIA – for example, where the data subject has consented, disclosure is necessary for contract performance, or it is required by law.

AfriForum ensures that all third-party recipients (including service providers and partners) are bound by written agreements that require compliance with POPIA's security and confidentiality provisions.

No personal information is transferred outside the Republic of South Africa unless adequate data-protection safeguards are in place as contemplated in section 72 of POPIA.

8.4 Planned transborder flows of personal information

AfriForum NPC makes limited use of transborder transfers of personal information, primarily for information storage, communication, and cloud-based services that support its administrative and membership operations.

All transfers are carried out in accordance with Section 72 of the Protection of Personal Information Act (POPIA) and only to countries, or under contracts, that provide adequate data-protection safeguards substantially similar to those contained in POPIA.

Purpose of Processing / Function	Country or Region Where Data May Be Stored or Accessed	Categories of Personal Information Affected	Lawful Basis / Safeguard
Cloud-based data storage and backup (email, document management, collaboration tools)	Primarily in the European Union (Ireland / Netherlands) and United States (via service providers such as Microsoft 365, Google Workspace, or equivalent)	Employee contact details, internal correspondence, administrative and project documents containing member or volunteer information	Data-processing agreements ensuring POPIA-compliant safeguards and alignment with EU GDPR adequacy standards
Website hosting and analytics	European Union (EU data centres) and United States (content-delivery networks and analytics providers)	Website user data, cookies, browser and usage statistics	Standard Contractual Clauses (SCCs) and POPIA-compliant privacy undertakings with service providers
Email marketing and member communication platforms	European Union and United States	Names, email addresses, membership status, communication preferences	Explicit consent by members/subscribers; provider contracts guaranteeing equivalent protection
Payment processing (online donations or membership fees)	South Africa (PayFast / local gateway) – some card processors may transmit via EU/UK for clearing	Limited financial identifiers (name, card or transaction reference, amount)	Processed under secure, PCI-DSS-compliant systems; contractual protection and local compliance

Website or server backups managed by third-party IT providers	EU or other secure jurisdictions with POPIA-equivalent protections	Technical system backups that may contain limited personal information	Data-processing agreements with confidentiality and security clauses

AfriForum does not intentionally transfer or sell personal information to any foreign entities for marketing or profiling purposes.

All third-party processors handling information outside South Africa are bound by written data-processing agreements incorporating POPIA-compliant terms and international security standards.

Transborder transfers are made only when necessary for legitimate organisational functions such as cloud hosting, communication, or payment processing.

Data subjects are informed of the possibility of such transfers through AfriForum's Privacy Notice and Website Policy.

8.5 General description of Information Security Measures to be implemented by

the responsible party to ensure the confidentiality, integrity and availability of

the information.

AfriForum NPC recognises its obligations under Section 19 of the *Protection of Personal Information Act 4 of 2013* (POPIA) to secure the integrity and confidentiality of all personal information in its possession or under its control.

To that end, AfriForum has implemented a combination of technical, administrative, and physical safeguards designed to prevent loss, unauthorised access, disclosure, alteration, or destruction of personal information.

A. Organisational and Administrative Controls

- Appointment of an Information Officer and Deputy Information Officers formally delegated in writing.

- Adoption of a Data-Protection and Information-Security Policy governing how information is collected, stored, shared, and destroyed.

- Regular staff awareness and POPIA training programmes for all employees, volunteers, and contractors handling personal data.

- Confidentiality undertakings included in employment contracts and service-provider agreements.

- Periodic risk assessments and compliance audits to identify vulnerabilities and test the effectiveness of controls.

- Defined incident-response and breach-notification procedures in line with Section 22 of POPIA.

B. Physical and Environmental Security

- Controlled access to AfriForum premises through reception sign-in, visitor logs, and restricted-area entry.

- Secure filing cabinets and lockable storage for paper-based records containing personal or financial data.

- 24-hour alarm and CCTV systems at head office and regional facilities, monitored through authorised community-safety and dedicated security channels.

- Document-destruction protocol using shredding or certified disposal for obsolete physical records.

C. Information-Technology and Technical Safeguards

- Role-based access controls and user authentication (password and multi-factor verification) for all systems containing personal information.

- Encryption of data at rest and in transit, including secure (HTTPS/TLS) communication for websites and email servers.

- Deployment of enterprise-grade antivirus, anti-malware, and firewall protection on all endpoints and servers.

- Regular patch management and software updates across the IT environment.

- Network segmentation and limited administrative privileges to reduce internal-threat exposure.

- Secure backup and recovery systems, including encrypted cloud backups stored in compliant data centres (EU/SA).

- Continuous monitoring and logging of system activity to detect and investigate unauthorised access attempts.

- Data-loss-prevention (DLP) and email-filtering tools to prevent leakage of sensitive information.

D. Third-Party and Cloud Security

- All third-party service providers (including IT, payroll, hosting, and communication platforms) are bound by written data-processing agreements ensuring POPIA-compliant security standards.

- Providers are vetted for compliance.

- Regular contract reviews confirm continued adherence to AfriForum's data-protection requirements.

E. Data Retention and Disposal

- Personal information is retained only for as long as necessary to achieve the lawful purpose of processing or as required by law.

- Secure deletion of electronic data and destruction of physical records are performed in accordance with AfriForum's Records Retention and Disposal Policy.

F. Business Continuity and Availability Measures

- Maintenance of redundant backup systems and off-site storage for critical data.

- Documented Business Continuity and Disaster Recovery Plan to restore systems and data in the event of interruption or cyber incident.

- Regular testing of recovery procedures to ensure minimal downtime and data loss.

Summary Statement

AfriForum continually reviews and enhances its information-security framework to ensure ongoing compliance with POPIA, PAIA, and generally accepted information-security standards.

All staff and partners are required to uphold these safeguards to maintain the confidentiality, integrity, and availability of personal information under AfriForum's control.

9. AVAILABILITY OF THE MANUAL

9.1 A copy of the Manual is available

    9.1.1   on https://afriforum.co.za/ ,

    9.1.2 at the head office of AfriForum (NPO) for public inspection during normal business hours;

    9.1.3 to any person upon request and upon the payment of a reasonable prescribed fee; and

    9.1.4 to the Information Regulator upon request.

9.2   A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

10. UPDATING OF THE MANUAL

The head of AfriForum (NPO) will on a regular basis update this manual.

Issued by

_____

CARL MARTIN KRIEL

Chief Executive Officer)