THIS

PAIA MANUAL

of

Name	Transport Cooling Africa Proprietary Limited
Registration Number	2022/713927/07
hereinafter “the Company”	

This PAIA Manual is executed in accordance with the provisions of PAIA read together with POPIA.

1. **INTERPRETATION AND DEFINITIONS**

1.1 Unless otherwise stated in this PAIA Manual:

1.1.1 The headings used in any clause will not be used in the interpretation of that clause;

1.1.2 Words or expressions defined in a clause of this PAIA Manual shall bear the same meaning throughout the entirety of this PAIA Manual;

1.1.3 Any reference to the term “written notice" shall include notice given by way of Electronic Communication.

1.2 Any word, term, definition, phrase or expression used anywhere in this PAIA Manual shall: include all genders; refer to natural persons and juristic persons; and the singular shall include the plural.

DEFINITIONS:

1.3 **Access Request**	refers to a formal written or electronic application submitted by a Requester seeking access to specified Records held by the Company.
1.4 **Board**	refers to the Board of directors of the Company as appointed and constituted from time to time.
1.5 **Company**	refers to Transport Cooling Africa Proprietary Limited with registration number: 2022/713927/07. The Company is a duly incorporated private company as envisaged in Section 8(2)(b) of the Companies Act No. 71 of 2008.
1.6 **Consent**	refers to any voluntary, specific, and informed expression of will in terms of which permission is given for the Processing of Personal Information.
1.7 **Data Subject**	refers to the individual or juristic person to whom the Personal Information relates.
1.8 **Deputy Information Officer**	refers to the person appointed to assist the Information Officer and act in their absence.
1.9 **Electronic Communication**	shall have the meaning ascribed thereto in Section 1 of the Electronic Communications and Transactions Act No. 25 of 2002.

1.10 **Head of the Company**	refers to the person in control of the Company, the Managing Director or Chief Executive Officer, responsible for ensuring compliance with PAIA.
1.11 **Information Officer**	refers to the person appointed by the Company to ensure compliance with POPIA and PAIA, who is responsible for overseeing data protection measures and serves as the liaison with the Information Regulator and Data Subjects.
1.12 **Information Regulator**	refers to the independent statutory body established in terms of Section 39 of POPIA. The Information Regulator is empowered to monitor and enforce compliance with both the POPIA and PAIA by public and private bodies in South Africa. Its functions include investigating complaints, conducting audits, issuing enforcement notices, and promoting awareness of data protection and access to information rights.
1.13 **Operator**	refers to a third party who processes Personal Information on behalf of the Company but does not decide on the purpose or means of Processing.
1.14 **PAIA**	refers to the Promotion of Access to Information Act, 2000 including all schedules, regulations and promulgations made thereunder from time to time.
1.15 **PAIA Manual**	refers to the PAIA Manual of the Company recorded in this document.
1.16 **Personal Information**	refers to any information relating to an identifiable, living natural person or a juristic person, including but not limited to names, contact details, identity numbers, biometric data, health or financial information, opinions, or correspondence.
1.17 **POPIA**	refers to the Protection of Personal Information Act No. 4 of 2013 including any regulations, schedule or promulgation made thereunder from time to time.
1.18 **POPIA Guide**	refers to the Company's internal POPIA compliance policies and/or procedures recorded in the POPIA Guide of the Company.
1.19 **Processing**	refers to any operation or set of operations performed on Personal Information, whether or not by automated means, including collection, receipt, recording, organization, storage, updating, retrieval, use, dissemination, or destruction

1.20 **Public Body**	refers to Government institutions subject to PAIA (distinct from private bodies like the Company).
1.21 **Record**	refers to any recorded information regardless of form or medium, including paper documents, electronic files, emails, photographs, videos, sound recordings, or any other format.
1.22 **Requester**	refers to the individual or legal entity submitting an Access Request under PAIA.
1.23 **Responsible Party**	refers to the Company in its capacity as the entity that determines the purpose and means of Processing Personal Information for the purposes of this document.
1.24 **SAHRC**	refers to the South African Human Rights Commission as established under Section 181 of the Constitution of the Republic of South Africa, 1996.

2. INTRODUCTION AND PURPOSE

INTRODUCTION

2.1 PAIA is a critical legislative instrument that operationalizes the constitutional right of access to information as guaranteed by Section 32 of the Constitution of South Africa. PAIA promotes transparency, accountability, and good governance by enabling individuals, organisations, and the public to request access to records held by both public and private bodies.

2.2 The Company recognises the importance of this right and is committed to facilitating lawful access to its records in a manner that balances transparency with the protection of privacy, commercial confidentiality, and other legitimate interests. This PAIA Manual is compiled in compliance with Section 51 of PAIA and the PAIA Regulations, and it complements the Company's obligations under POPIA.

2.3 All private bodies, including the Company, are legally required to compile, maintain, and publish a PAIA Manual. This manual must be made accessible to the public and regularly updated to reflect any changes in records management, contact details, or legislative amendments. Failure to comply may result in penalties, including fines or imprisonment, as stipulated under Section 90 of PAIA.

2.4 The manual serves as a practical guide for all stakeholders being customers, employees, suppliers, regulators, and the general public on how to access information held by the Company, the types of records available, and the procedures to follow in respect of such access to records held by the Company.

PURPOSE

2.5 The primary purpose of this PAIA Manual is to promote a culture of transparency, accountability and good governance within the Company by providing the public and all stakeholders with clear and accessible information about:

2.5.1 The nature and categories of Records held by the Company that may be accessed, either without a formal request or upon submission of a PAIA request;

2.5.2 How to make a request for access to Records, including detailed procedures, timelines and fees applicable under PAIA;

2.5.3 The contact details of the Information Officer and Deputy Information Officer, who are responsible for assisting Requesters and managing Access Requests in compliance with PAIA and POPIA;

2.5.4 The grounds on which access to Records may be refused, including justifiable limitations such as the protection of privacy, commercial confidentiality, legal privilege and security interests;

2.5.5 The remedies available to Requesters, including the right to lodge internal appeals and seek external review by the Information Regulator or courts (as applicable);

2.5.6 The Company's commitment to balancing openness with the protection of Personal Information and other legitimate interests, thereby ensuring compliance with both PAIA and POPIA;

2.5.7 How this PAIA Manual supports the realisation of South Africa's constitutional goals of an open, participatory democracy where all persons have effective access to information necessary to exercise and protect their rights;

2.5.8 The services and assistance available to the public to facilitate access to information in a manner that is as swift, inexpensive and effortless as reasonably possible;

2.5.9 Information about the Processing of Personal Information by the Company, including the categories of Data Subjects and Personal Information Processed, and any cross-border transfers thereof, in line with POPIA requirements;

2.5.10 The security measures implemented by the Company to ensure the confidentiality, integrity, and availability of information Processed and accessed.

2.6 This PAIA Manual is intended to serve as a practical and user-friendly guide for members of the public, employees, customers, suppliers, regulators and other stakeholders to understand their rights and the Company's obligations under PAIA. It fosters a culture of openness and accountability while respecting privacy and commercial sensitivities.

2.7 By making this PAIA Manual publicly available, the Company affirms its commitment to transparency and good governance, thereby enabling individuals and organisations to participate meaningfully in democratic processes and to protect their rights through informed access to information.

3. THE COMPANY'S PROMOTION OF ACCESS TO INFORMATION

HEAD OF THE COMPANY

3.1 The Head of the Company holds ultimate accountability for ensuring that the Company complies with its obligations under both PAIA and POPIA.

3.2 Under PAIA, the Head of the Company is recognised as the "head of the private body" and is responsible for:

3.2.1 Ensuring that the Company compiles, maintains, and makes available a compliant PAIA Manual as required by law;

3.2.2 Overseeing the implementation of policies and procedures that facilitate lawful access to information;

3.2.3 Ensuring that the Company Processes Access Requests in accordance with PAIA timelines and requirements;

3.2.4 Balancing the constitutional right of access to information with the protection of privacy, confidentiality and commercial interests;

3.2.5 Supporting the Information Officer and Deputy Information Officer (as applicable) in fulfilling their duties;

3.2.6 Ensuring that the Company complies with POPIA's conditions for lawful Processing of Personal Information, including security safeguards and Data Subject rights;

3.2.7 Authorising the appointment of the Information Officer and Deputy Information Officer and delegating responsibilities where appropriate.

3.3 The contact details of the Head of the Company are provided for later in this PAIA Manual for ease of reference.

INFORMATION OFFICER

3.4 The Information Officer is the designated individual responsible for the day-to-day management of the Company's compliance with PAIA and POPIA. This role is critical in ensuring that the Company meets its legal obligations and that data subjects' rights are respected.

3.5 Key responsibilities of the Information Officer include:

3.5.1 Receiving, processing and responding to PAIA requests within the statutory time period;

3.5.2 Advising Requesters on the procedure for accessing Records and the applicable fees;

3.5.3 Maintaining the PAIA Manual and ensuring it is regularly updated and accessible to the public;

3.5.4 Overseeing the implementation of POPIA compliance measures, including data protection policies, security controls and staff training;

3.5.5 Managing data breach incidents and ensuring timely notification to the Information Regulator and affected Data Subjects, as required by POPIA.

3.5.6 Liaising with the Information Regulator and other relevant authorities on matters relating to PAIA and POPIA compliance;

3.5.7 Ensuring that internal appeals against refusals of access are handled efficiently and fairly;

3.5.8 Keeping detailed records of all PAIA requests, responses, appeals, and POPIA compliance activities for audit and reporting purposes;

3.5.9 Promoting awareness and understanding of PAIA and POPIA within the Company through training and communication.

3.6 The Information Officer's contact details are provided later in this PAIA Manual.

DEPUTY INFORMATION OFFICER

3.7 The Deputy Information Officer assists the Information Officer in fulfilling the Company's PAIA and POPIA obligations and acts in their stead during periods of absence or unavailability.

3.8 Responsibilities of the Deputy Information Officer include:

3.8.1 Supporting the Information Officer in receiving and processing PAIA requests and appeals;

3.8.2 Assisting with the maintenance and dissemination of this PAIA Manual;

3.8.3 Participating in the management of POPIA compliance initiatives, including data protection impact assessments and breach response;

3.8.4 Providing training and awareness sessions to staff regarding their obligations under PAIA and POPIA;

3.8.5 Ensuring continuity of compliance efforts and acting as a liaison with the Information Regulator when required.

SAHRC

3.9 In terms of PAIA, the SAHRC plays a pivotal role in supporting and promoting the constitutional right of access to information as enshrined in Section 32 of the Constitution. The SAHRC's obligations under PAIA include:

3.9.1 Promoting the Right of Access to Information: The SAHRC actively promotes awareness and understanding of PAIA rights among the public, particularly focusing on educating disadvantaged and vulnerable groups to enable them to exercise their rights effectively;

3.9.2 Monitoring Implementation and Compliance: The SAHRC monitors how public and private bodies comply with PAIA, including the submission of annual reports on Access Requests and responses. It assesses the effectiveness of PAIA in promoting transparency and accountability;

3.9.3 Providing Assistance to Requesters: Where reasonably possible, the SAHRC assists individuals who wish to exercise their rights under PAIA, including guidance on how to submit requests and navigate the appeal processes;

3.9.4 Conducting Education and Outreach: The SAHRC develops and conducts educational programs and campaigns to advance public understanding of PAIA and the right of access to information. This includes workshops, publications, and community engagement initiatives;

3.9.5 Making Recommendations for PAIA Reform: The SAHRC advises government and Parliament on legislative and policy reforms to improve PAIA's effectiveness and ensure it remains fit for purpose in the evolving information age;

3.9.6 Reporting to Parliament: The SAHRC submits annual reports to Parliament detailing its activities, findings, and recommendations regarding PAIA implementation and human rights observance.

3.10 Transition of PAIA Functions to the Information Regulator: Following the enactment of POPIA and the establishment of the Information Regulator, certain functions relating to PAIA enforcement and complaints handling have been transferred from the SAHRC to the Information Regulator. However, the SAHRC retains its constitutional mandate to promote, protect, and monitor the right of access to information as a fundamental human right.

3.11 How the SAHRC supports the Company and the public include:

3.11.1 The SAHRC provides guidance and resources to assist private bodies like the Company in complying with PAIA, including training materials and best practice manuals;

3.11.2 It offers a platform for members of the public to lodge complaints regarding access to information issues and human rights violations related to information access;

3.11.3 The SAHRC's website and offices serve as accessible points for information dissemination and assistance related to PAIA.

4. PERSONAL INFORMATION PROCESSING BY THE COMPANY

4.1 The Company is committed to Processing Personal Information lawfully, transparently, and securely in compliance with POPIA and related legislation. The Company Processes Personal Information only where a lawful basis exists and in accordance with the principles set out in POPIA and the Company's POPIA Guide which may be obtained via a formal request, which include accountability, Processing limitation, purpose specification, further Processing limitation, information quality, openness, security safeguards, and Data Subject participation.

4.2 The Company's lawful Processing and legal adherence include:

4.2.1 Lawfulness, fairness, and transparency: Personal Information is Processed lawfully and fairly, and Data Subjects are informed of the purposes and manner of Processing;

4.2.2 Consent: Where applicable, the Company obtains the Data Subject's informed, specific, and voluntary Consent prior to Processing Personal Information, except where Processing is justified under other lawful bases such as contractual necessity, legal obligation, or legitimate interests;

4.2.3 Collection directly from Data Subjects: Personal Information is collected directly from the Data Subject wherever reasonably practicable, ensuring accuracy and completeness;

4.2.4 Minimality: Only Personal Information that is adequate, relevant, and not excessive in relation to the purpose for which it is processed is collected and retained;

4.2.5 Purpose specification: Personal Information is collected for specific, explicitly defined, and legitimate purposes and is not further Processed in a manner incompatible with those purposes for which it is collected;

4.2.6 Retention and destruction: Personal Information is retained only for as long as necessary to fulfil the purpose of collection or to comply with legal obligations, after which it is securely destroyed or anonymized;

4.2.7 Security safeguards: Appropriate technical and organizational measures are implemented to protect Personal Information against loss, damage, unauthorized access, or unlawful Processing;

4.2.8 Data Subject rights: The Company respects and facilitates Data Subject rights including access, correction, deletion, objection to Processing, and withdrawal of Consent where applicable.

4.3 The Company's Processing activities include collection, receipt, recording, organization, storage, updating, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction of Personal Information, as necessary to conduct its business operations and comply with legal obligations. The Company maintains records of Processing activities as required by POPIA and ensures ongoing compliance through regular audits, staff training, and data protection impact assessments.

4.4 The Company undertakes to implement such further and enhanced protection measures as necessary if dealing with special forms of Personal Information such religious and beliefs information, information of a minor (below the age of 18 years) and such further special information as stipulated by PAIA, POPIA or other legislation or regulations.

RETENTION OF PERSONAL INFORMATION

4.5 The Company acknowledges its responsibility to manage Personal Information in compliance with POPIA, particularly regarding the retention and destruction of Personal Information.

4.6 The Company's Personal Information retention principles and rights include the following:

4.6.1 Purpose Limitation: Personal Information shall only be retained for as long as is necessary to achieve the purpose for which it was collected or subsequently Processed in accordance with the provisions of POPIA;

4.6.2 Retention Period: In line with industry standards and applicable legislation, the Company retains Personal Information for a period not exceeding 7 (seven) years from the date that the information was last used or the relevant transaction was completed, unless a longer or shorter retention period is required or authorized by law, contract, or Consent;

4.6.3 Legal and Contractual Obligations: The Company may retain Personal Information beyond 7 (seven) years where retention is necessary for the defence or enforcement of legal claims;

4.6.4 Consent for Extended Retention: Where applicable, the Company will obtain explicit Consent from the Data Subject to retain Personal Information beyond the standard retention period;

4.6.5 Secure Destruction: Upon expiry of the retention period or upon the Company no longer being authorized to retain the information, Personal Information will be destroyed, deleted, or de-identified as soon as reasonably practicable in a manner that prevents reconstruction in an intelligible form;

4.6.6 Data Subject Requests: Upon receipt of a valid request from a Data Subject for deletion or destruction of their Personal Information, the Company will assess the request in accordance with POPIA and applicable laws. If no lawful basis exists to retain the information, the Company will promptly comply with the deletion or destruction request;

4.6.7 Retention for historical, statistical, or research purposes: The Company may retain Personal Information beyond the retention period for these purposes, provided appropriate safeguards are in place to prevent use for other purposes.

4.7 The Company's Record keeping periods and accountability includes the following:

4.7.1 The Company maintains a Records' retention schedule detailing retention periods for different categories of Personal Information;

4.7.2 Regular audits and reviews are conducted to ensure compliance with retention policies; and

4.7.3 All employees and third-party Operators Processing Personal Information on behalf of the Company are required to comply with these retention policies.

4.8 PROCESSING LIMITATIONS

4.8.1 The Company adheres strictly to the principle of purpose limitation as required by POPIA, meaning that Personal Information collected for a single purpose shall not be further Processed in a manner incompatible with that original purpose.

4.8.2 General limitations on Processing includes the following:

4.8.2.1 No incompatible Processing: The Company will not Process Personal Information for purposes other than those explicitly specified and communicated to the Data Subject at the time of collection, unless the further Processing is compatible with the original purpose;

4.8.2.2 Data Subject notification: Where further Processing is contemplated, the Company will inform the Data Subject of the new purpose and obtain Consent if required;

4.8.2.3 Data minimization: Further Processing activities will be limited to what is necessary and proportionate to the new purpose.

4.8.3 Circumstances which shall justify the further Processing of Personal Information by the Company shall include the following:

4.8.3.1 With Data Subject Consent: The Data Subject has given explicit Consent to the new Processing purpose;

4.8.3.2 Legal or regulatory requirement: Processing is required or authorized by law or regulation;

4.8.3.3 Contractual necessity: Further Processing is necessary to fulfil a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into a contract;

4.8.3.4 Legitimate interests: The Company has a legitimate interest in further Processing that is not overridden by the interests, rights, or freedoms of the Data Subject, and appropriate safeguards are in place;

4.8.3.5 Public interest or research: Further Processing is necessary for historical, statistical, or research purposes, subject to safeguards to protect Data Subjects' rights.

4.8.4 Restrictions and safeguards by the Company:

4.8.4.1 The Company will ensure that any further Processing complies with all POPIA conditions, including security safeguards, Data Subject rights, and accountability obligations;

4.8.4.2 If the further Processing is incompatible with the original purpose and no lawful basis exists, the Company will not proceed with such further Processing; and

4.8.4.3 The Company will document and justify all instances of further Processing to demonstrate compliance with POPIA.

QUALITY UNDERTAKING

4.9 The Company is committed to ensuring the quality of all Personal Information it collects, stores, and processes, in compliance with the provisions of POPIA.

4.10 The Company takes all reasonably practicable steps to ensure that Personal Information is:

4.10.1 Complete: All necessary data to fulfil the purpose for which Personal Information is collected;

4.10.2 Accurate: Information in the Company's possession is ensured to be correct and free from errors;

4.10.3 Not Misleading: Data is truthful and not presented in a way that could mislead; and

4.10.4 Up to Date: Information is regularly reviewed and updated as necessary to maintain accuracy.

4.11 The Company assesses the quality of Personal Information in light of the purpose for which the information was collected or is further Processed to ensure relevance and adequacy.

4.12 Procedures such as data verification at collection, periodic audits, and updates through communication with Data Subjects are implemented to maintain data quality.

4.13 Inaccurate or outdated Personal Information identified by the Company or notified by Data Subjects will be corrected or deleted without undue delay.

4.14 The Company ensures that personal information collected from third parties is verified for accuracy and completeness before Processing.

5. PERSONAL INFORMATION PROCESSING PURPOSES

5.1 The Company Processes Personal Information for distinct purposes depending on the category of the Data Subject. These purposes are lawful, specific, and communicated to Data Subjects at the point of collection or as soon as reasonably possible thereafter.

5.2 Clients and Prospective Clients

5.2.1 Purpose: To provide products and services, manage client relationships, process transactions, respond to inquiries, conduct marketing and customer support, and comply with contractual and legal obligations.

5.2.2 Examples: Processing contact details, financial information, transaction history, and communication records.

5.2.3 Legal basis: Consent, contractual necessity, or legal interests such as fraud prevention or credit checks.

5.3 Employees and Contractors

5.3.1 Purpose: To manage employment relationships, effect payroll, benefits administration, performance management, training, health and safety compliance, and statutory reporting.

5.3.2 Examples: Processing personal identification, employment contracts, banking details, medical records (where applicable), and disciplinary records.

5.3.3 Legal basis: Contractual necessity, legal obligation, and legal interests such as workplace safety.

5.4 Suppliers and Service Providers

5.4.1 Purpose: To manage procurement, contracts, payments, compliance monitoring, and communication.

5.4.2 Examples: Processing company details, contact persons, banking information, and contractual documents.

5.4.3 Legal basis: Contractual necessity.

5.5 Other Companies and Business Partners

5.5.1 Purpose: For strategic partnerships, joint ventures, compliance with regulatory requirements, and business development.

5.5.2 Examples: Processing corporate contact information, contractual agreements, and compliance documentation.

5.5.3 Legal basis: Contractual necessity.

5.6 General Public and Website Users

5.6.1 Purpose: To provide information, respond to inquiries, manage website based interactions, and improve online services.

5.6.2 Examples: Processing contact details, IP addresses, and usage data.

5.6.3 Legal basis: Consent for marketing communications and legislative requirements.

5.7 The Company shall collect and Process various forms of Personal Information from different categories of Data Subjects which Personal Information shall differ depending on the categories of the Data Subjects and the purpose for which the Personal Information is collected and Processed by the Company, the categories of Data Subjects shall include but not be limited to:

5.7.1 CLIENTS

5.7.1.1 For clients, the Company collects Personal Information necessary to establish and maintain the business relationship, provide services, and comply with legal obligations. This includes:

5.7.1.1.1 Identification details: Full name, date of birth, gender, nationality, identity number or passport number;

5.7.1.1.2 Contact information: Physical address, postal address, telephone numbers, email addresses, and other online identifiers;

5.7.1.1.3 Financial information: Bank account details, credit history, payment records, transaction details;

5.7.1.1.4 Demographic information: Marital status, employment status, occupation;

5.7.1.1.5 Communication records: Correspondence, service requests, complaints, and feedback.

5.7.1.1.6 Special personal information (if applicable): Health information (for insurance or medical-related services), biometric data (e.g., fingerprint or facial recognition for authentication).

5.7.1.1.7 Consent and preferences: Marketing preferences, Consent records for processing and communications.

5.7.2 SUPPLIERS AND/OR CONTRACTORS

5.7.2.1 The Company collects Personal Information from suppliers and contractors to manage procurement, contracts, and compliance:

5.7.2.1.1 Company and representative details: Business registration number, VAT number, contact persons' names and identification numbers;

5.7.2.1.2 Contact information: Physical and postal addresses, telephone numbers, email addresses;

5.7.2.1.3 Banking and payment details: Bank account numbers, payment terms, tax clearance certificates;

5.7.2.1.4 Contractual information: Signed agreements, service level agreements, performance records.

5.7.2.1.5 Compliance information: Health and safety certifications, insurance details, legal compliance documents.

5.7.3 THIRD PARTY OPERATORS

5.7.3.1 Third party operators engaged by the Company to Process Personal Information on its behalf provide information necessary for contract management and oversight:

5.7.3.1.1 Operator identification: Company registration details, contact person names and identification.

5.7.3.1.2 Contact information: Addresses, telephone numbers, emails.

5.7.3.1.3 Contractual and operational data: Service agreements, compliance certifications, audit reports.

5.7.3.1.4 Security and access details: User access logs, incident reports related to Personal Information Processing.

5.7.4 EMPLOYEES AND PROSPECTIVE EMPLOYEES

5.7.4.1 The Company collects extensive Personal Information from employees and job applicants for recruitment, employment, and statutory compliance:

5.7.4.1.1 Identification and demographic details: Full name, date of birth, gender, nationality, identity number or passport number.

5.7.4.1.2 Contact information: Physical and postal addresses, telephone numbers, email addresses.

5.7.4.1.3 Employment history: Curriculum vitae, references, qualifications, previous employment records.

5.7.4.1.4 Payroll and benefits: Bank account details, tax numbers, pension and medical aid information.

5.7.4.1.5 Health and safety: Medical records, disability status, occupational health data.

5.7.4.1.6 Performance and disciplinary records: Appraisals, warnings, grievances, training records.

5.7.4.1.7 Special personal information: Biometric data (such as fingerprint for access control), union membership, religious beliefs (where voluntarily disclosed).

5.7.4.1.8 Consent and emergency contacts: Consent for Processing, next of kin details.

5.7.5 VARIOUS FURTHER CATEGORIES OF DATA SUBJECTS

5.7.5.1 The Company may also Process Personal Information from other categories of Data Subjects, including but not limited to:

5.7.5.1.1 Visitors and contractors on Company premises: Identification, access logs, vehicle registration details.

5.7.5.1.2 Website users and online service users: IP addresses, cookies, device identifiers, browsing behaviour, contact details submitted via online forms.

5.7.5.1.3 Regulatory bodies and government agencies: Correspondence, compliance documentation, audit information.

5.7.5.1.4 Marketing and event participants: Contact details, preferences, Consent records, participation history.

6. DATA SUBJECT'S CONSENT OR OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

CONSENT

6.1 In accordance with the provisions of POPIA, the Company Processes Personal Information only where the Data Subject or a competent person (in the case of a child) has given valid Consent, unless another lawful basis for Processing applies.

6.2 POPIA defines Consent as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information." This means the key requirements that the Company will implement and adhere to when obtaining Consent shall include:

6.2.1 The Company shall clearly specify the purpose(s) for which Personal Information will be Processed at or before the time of collection by the Company;

6.2.2 The Data Subject will be notified of their rights under POPIA, including the right to withdraw Consent at any time;

6.2.3 Consent will be obtained in writing, electronically, verbally, or by any other means that clearly demonstrates the Data Subject's intention;

6.2.4 The Company shall not assume Consent or infer such from silence or pre-ticked boxes, the Company shall implement active affirmation; and

6.2.5 Where Personal Information is collected from a third party, the Company shall ensure that the Data Subject has Consented to such collection and Processing.

6.3 *Withdrawal of Consent*

6.3.1 The Data Subject may withdraw Consent at any time by notifying the Company thereof in writing.

6.3.2 Withdrawal does not affect the lawfulness of Processing conducted by the Company prior to the date of the withdrawal. Upon withdrawal, the Company will cease Processing the Personal Information unless the Company is required by any applicable law to continue such Processing of Personal Information of the Data Subject.

OBJECTION

6.4 In terms of POPIA, a Data Subject has the right to object to the Processing of their Personal Information at any time on reasonable grounds relating to their particular situation, except where legislation expressly authorizes such Processing.

6.5 How to object:

6.5.1 The objection must be made in the prescribed manner, which for the Company means:

6.5.1.1 Submitting a written objection to the Company's Information Officer or designated contact point; and

6.5.1.2 Clearly stating the grounds for objection and identifying the Processing activities concerned.

6.5.2 The Company will acknowledge receipt of the objection and respond within a reasonable timeframe from the date that the objection is received by the Company.

6.6 Requirements for a valid objection:

6.6.1 The objection must be based on reasonable grounds related to a Data Subject's specific circumstances, such as privacy concerns, incorrect or excessive Processing;

6.6.2 The objection must be specific to certain Processing activities and not a general refusal;

6.6.3 The objection must be made in good faith and not for purposes of evading legitimate contractual or legal obligations.

6.7 Consequences of an objection:

6.7.1 Upon receipt of a valid objection, the Company may no longer process the personal information for the objected purposes unless:

6.7.1.1 The Company demonstrates compelling legitimate grounds that override the Data Subject's interests, rights, and freedoms; or

6.7.1.2 Processing is necessary for the establishment, exercise, or defence of a legal claim; or

6.7.1.3 Processing is required by law.

6.7.2 If the objection is upheld, the Company will cease Processing and take reasonable steps to delete, anonymize, or restrict the Personal Information as appropriate.

6.7.3 If the objection is overridden, the Company will inform the Data Subject of the reasons and any recourse available.

6.8 Objection in relation to direct marketing:

6.8.1 Data Subjects have an unconditional right to object to Processing for direct marketing purposes, including profiling related to direct marketing.

6.8.2 The Company will immediately cease processing for direct marketing upon objection without requiring justification.

7. DATA SUBJECT'S ACCESS TO PERSONAL INFORMATION

7.1 Data Subjects have the constitutional and statutory right to access their Personal Information held by the Company, as provided for in Section 23 of POPIA and PAIA.

7.2 RIGHT TO ACCESS

7.2.1 Data Subjects may request access to their Personal Information by submitting a formal request to the Company's Information Officer as outlined in this PAIA Manual;

7.2.2 The Company will respond within 30 (thirty) calendar days of receipt of the request, providing access in a reasonable manner, being by means of inspection, making copies, or electronic format;

7.2.3 The Company will inform the Data Subject of any fees payable for Processing the Access Request in accordance with PAIA's prescribed tariffs; and

7.2.4 Access may be restricted or refused only on lawful grounds, including protection of third-party privacy or commercial confidentiality, with reasons to be communicated in writing by the Company to the Data Subject requesting so access.

7.3 CORRECTION AND DELETION

7.3.1 Data Subjects may request correction, deletion, or destruction of their Personal Information if it is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or unlawfully obtained; and

7.3.2 The Company will assess such requests and take appropriate action within a reasonable time, balancing Data Subject rights with legal and operational requirements.

7.4 ASSISTANCE AND TRANSPARENCY

7.4.1 The Company's Information Officer will assist Data Subjects in exercising their access rights and provide guidance on the process; and

7.4.2 Contact details and procedures for Access Requests are provided later in this PAIA Manual.

8. THE COMPANY'S SAFETY MEASURES

8.1 The Company implements appropriate technical and organizational measures to safeguard any form of Personal Information in its possession, which safety measures are consistent with the requirements of POPIA.

8.2 PHYSICAL SECURITY

8.2.1 Controlled access to Company premises and secure storage facilities; and

8.2.2 Visitor management and restricted access areas for sensitive records.

8.3 TECHNICAL SECURITY

8.3.1 Use of firewalls, encryption, anti-malware, and intrusion detection systems;

8.3.2 Secure authentication methods including multi-factor authentication for system access; and

8.3.3 Regular software updates and vulnerability assessments.

8.4 ACCESS CONTROLS

8.4.1 Role-based access permissions limiting Personal Information access to authorized personnel only; and

8.4.2 Logging and monitoring of access to Personal Information systems.

8.5 DATA INTEGRITY AND CONFIDENTIALITY

8.5.1 Measures to prevent unauthorized alteration, loss, or destruction of Personal Information; and

8.5.2 Secure backup and disaster recovery procedures.

8.6 INCIDENT MANAGEMENT

8.6.1 Procedures for detecting, reporting, and responding to data breaches or security incidents; and

8.6.2 Notification protocols to the Information Regulator and affected Data Subjects as required by law.

8.7 STAFF TRAINING AND AWARENESS

8.7.1 Regular data protection training programs for all employees and contractors; and

8.7.2 Clear policies and disciplinary measures regarding data protection compliance.

8.8 THIRD-PARTY MANAGEMENT

8.8.1 Due diligence and contractual obligations imposed on service providers and operators Processing Personal Information on behalf of the Company to ensure compliance with POPIA security requirements.

8.9 CONTINUOUS IMPROVEMENT

8.9.1 Periodic risk assessments and audits to evaluate and enhance security measures; and

8.9.2 Implementation of corrective actions based on audit findings and evolving threats.

9. **COMPANY RECORDS**

VOLUNTARY DISCLOSURE AND AUTOMATIC AVAILABILITY OF RECORDS

9.1 In terms of Section 52(1) of PAIA, the Company (by means of the Head of the Company) may voluntarily publish a Section 52 Notice. This notice describes categories of Records that the Company makes available automatically and without the need for a formal request. The purpose of this provision is to promote transparency and reduce the administrative burden of processing routine Access Requests.

9.2 The Section 52 Notice includes: Records available for inspection without a formal request under other legislation or company policy; Records available for purchase or copying, such as brochures, policies, or standard contracts; and Records available free of charge, such as publicly accessible reports or notices.

9.3 The Company hereby confirms that it has not published any category of Records in terms of Section 52 of PAIA which is automatically made available to any person without a request.

RECORDS AVAILABLE UPON REQUEST

9.4 The following categories of Records of the Company require a formal PAIA request to be made available to any Requester, including but not limited to:

9.4.1 Corporate Governance Records such as: Board minutes, shareholder agreements and minutes, internal policies, incorporation documents, memorandum of incorporation, the security register and certificates, information regarding members of the Board and holders of the Company's securities.

9.4.2 Employee Records such as: Employment contracts, payroll information, disciplinary files, training documents, employees' information.

9.4.3 Customer and supplier records such as: Contracts/Agreements between the Company and a customer or supplier, purchase orders, correspondence, invoices, details regarding any supplier or customer, any information or Record supplied by a third party.

9.4.4 Operational Records such as: Project files, audit reports, risk assessments, IT system logs, advertising and promotional materials, product lists, supplier lists and contractor lists.

9.4.5 Personal Information such as: Any form of data of a customer, supplier or employee processed in terms of POPIA.

9.4.6 Financial Records such as: Audit reports, risk assessments and management plans, accounting records, annual financial statements, tax returns, financial policies and procedures, banking records/details/statements as well as debtor and creditor information.

9.4.7 Tax Records which shall include any form of taxation records of whatsoever nature.

9.4.8 Company policies such as: Health and Safety assessments/reports, grievance procedures, leave policies, training requirements and all forms of manuals.

9.4.9 IT related Records such as: IT systems, software, IT user agreements and policies and IT manuals.

9.4.10 Legal and privileged Records such as: Litigation files, legal opinions, and intellectual property documents.

9.5 Access to these records is subject to PAIA's procedural requirements and may be refused on statutory grounds.

RECORDS AVAILABLE WITHOUT A REQUEST AND IN TERMS OF OTHER LEGISLATION

9.6 Records which are of a public nature and freely accessible are made available without a PAIA request due in part to other legislation which mandates their disclosure. The aforementioned legislation shall include but not be limited to:

9.6.1 Companies Act No. 71 of 2008: Annual financial statements and shareholder information;

9.6.2 Income Tax Act No. 58 of 1962: Tax filings and related correspondence;

9.6.3 Labour Relations Act No. 66 of 1995: Collective agreements and dispute resolution records;

9.6.4 Basic Conditions of Employment Act No. 75 of 1997: Employment conditions and standards;

9.6.5 Occupational Health and Safety Act No. 85 of 1993: Health and safety compliance records;

9.6.6 National Environmental Management Act No. 107 of 1998: Environmental impact assessments and compliance reports;

9.6.7 Financial Intelligence Centre Act, 38 of 2001: Records related to anti-money laundering compliance.

9.7 Access to these records is governed by the relevant legislation and may be subject to PAIA where applicable.

PROCEDURE TO REQUEST ACCESS TO A RECORD OF THE COMPANY

9.8 In accordance with the provisions of Section 18 of PAIA, Requesters must complete the required forms and procedures so as to request access to Records of the Company, in addition to which the following steps are listed below;

9.8.1 STEP 1: SUBMISSION OF REQUEST

9.8.1.1 The request must be in writing (including email or electronic means) and signed by the Requester or its authorised agent;

9.8.1.2 The request must clearly identify the Record(s) sought with sufficient detail (e.g., date, subject, reference numbers);

9.8.1.3 The request must specify the form of access required: Such as inspection, copies, or electronic format;

9.8.1.4 The request must provide contact details for a response (address, email, or postal);

9.8.1.5 The request must state the right to be exercised or protected and explain why the Record is required for that purpose; and

9.8.1.6 The request must include payment of the prescribed request fee or proof of exemption (as applicable).

9.8.2 STEP 2: ACKNOWLEDGEMENT AND PROCESSING

9.8.2.1 The Company acknowledges receipt promptly and logs the request;

9.8.2.2 The Information Officer or delegated official processes the request within 30 (thirty) calendar days; and

9.8.2.3 If necessary, the Company may request further particulars to locate the Record.

9.8.3 STEP 3: RESPONSE

9.8.3.1 The Company will grant access, refuse access with reasons, or inform the Requester of fees payable; and

9.8.3.2 If fees are payable, Processing will commence once payment or deposit is received.

9.9 If for any reason such as disability or otherwise, the Requester is not able to perform the request in writing, he/she may be allowed to make such request in a verbal manner.

PRECONDITIONS FOR ACCESS TO RECORDS

9.10 Before access to Records may be considered and/or granted by the Company, the Requesters must:

9.10.1 Submit a compliant written request in accordance with the form and manners determined by PAIA and/or this PAIA Manual;

9.10.2 Pay the prescribed request fee in accordance with the provisions of Section 54 of PAIA, alternatively, provide proof of his/her exemption;

9.10.3 Pay any additional fees for search, reproduction, or access prior to receipt of Records;

9.10.4 Comply with any additional procedural requirements set forth in PAIA or this PAIA Manual.

9.11 Failure to adhere to the above stated preconditions may result in delayed or refused access to Records by the Company.

PAIA PRESCRIBED FEES

9.12 Fees related to any PAIA request or otherwise are regulated in accordance with the provisions of Sections 22 and 54 of PAIA, the Company hereby provides an estimate of the fees below together with an indication of any deposit amount required:

Activity	**FEE (ZAR)**
Request fee, payable by every Requester.	R140.00
Photocopy or printed black & white copy for every A4 page.	R2.00 per page or part of the page
Printed copy of A4-size page.	R2.00 per page or part of the page
For a copy in a computer-readable form on: a flash drive (provided by the Requester). a compact disc (CD) if the Requester provides the CD to us. a compact disc (CD) if we give the CD to the Requester.	 R40.00 R40.00 R60.00
For a transcription of visual images, for an A4-size page or part of the page.	This service will be outsourced. The fee will depend on the quotation from the service provider.
For a copy of visual images.	This service will be outsourced. The fee will depend on the quotation from the service provider.
For a transcription of an audio record, per A4-size page.	R24.00
For a copy of an audio record on a flash drive (provided by the Requester). For a copy of an audio record on compact disc (CD) if the Requester provides the CD to us. For a copy of an audio record on compact disc (CD) if we give the CD to the Requester.	R40.00 R40.00 R60.00
For each hour or part of an hour (excluding the first hour) reasonably required to search for, and prepare the record for disclosure.	R145.00

The search and preparation fee cannot exceed.	R435.00
Deposit – if the search exceeds 6 (six) hours.	One-third of the amount per request.
Postage, email or any other electronic transfer.	Actual expense, if any.

REFUSAL OF ACCESS TO A RECORD

9.13 A request for access to any Record held by the Company may be refused in terms of Chapter 4 of PAIA, for reasons which shall include but not be limited to:

9.13.1 Protect the privacy of third parties (Section 63 of PAIA);

9.13.2 Safeguard commercial information and trade secrets (Section 64 of PAIA);

9.13.3 Protecting confidential information of a third party (Section 65 of PAIA);

9.13.4 Maintain legal professional privilege (Section 67 of PAIA);

9.13.5 Protect research information of the Company or a third party (Section 69 of PAIA);

9.13.6 Protect the Company's rights and any form or part of its property (Section 66 of PAIA); and

9.13.7 Reasons of national security, public safety, or international relations (Section 70 of PAIA).

9.14 In the event that the Company refuses a Requester access to any Records of the Company, the Company shall provide the Requester with written reasons for such refusal, including the specific grounds and information and shall notify the Requester of the Requester's right to appeal such refusal.

AVAILABLE REMEDIES FOR WHEN ACCESS TO A RECORD IS REFUSED

9.15 <u>INTERNAL APPEAL (SECTION 74 OF PAIA)</u>

9.15.1 Procedure:

9.15.1.1 A Requester may lodge an internal appeal with the Head of the Company (or designated senior official) within 60 (sixty) calendar days of receiving the refusal notice; and

9.15.1.2 The appeal must be in writing, stating the grounds for appeal and referencing the original request.

9.15.2 Processing:

9.15.2.1 The Head of the Company must decide the appeal within 30 calendar days of receipt; and

9.15.2.2 If upheld, access is granted; if dismissed, written reasons referencing PAIA grounds for the dismissal must be provided.

9.15.3 Company commitment:

9.15.3.1 The Company will facilitate appeals transparently, providing guidance on a submission and will acknowledge receipt within 5 (five) business days.

9.16 EXTERNAL REVIEW (SECTIONS 78 TO 79 OF PAIA)

9.16.1 If dissatisfied with the internal appeal outcome, the Requester may apply to the Information Regulator within 60 (sixty) days from the date of dismissal in terms of an internal appeal.

9.16.2 The Information Regulator may investigate, mediate, or issue a binding determination.

9.16.3 Alternatively, the Requester may apply to a competent court for review. The court may order access, set aside the refusal, or award costs (as applicable).

DECISION MAKING OF THE COMPANY TO ALLOW OR REFUSE ACCESS TO RECORDS

9.17 The Head of the Company or delegated Information Officer will:

9.17.1 Assess the request against PAIA's procedural and substantive requirements;

9.17.2 Consult relevant departments or third parties as necessary;

9.17.3 Consider the Requester's rights, privacy concerns, confidentiality, and public interest;

9.17.4 Make a reasoned decision to grant or refuse access within the statutory 30 (thirty) day period; and

9.17.5 Communicate the decision in writing to the Requester, including reasons for refusal and appeal rights.

9.18 The Company shall ensure that all such decisions made in respect of PAIA are fair, consistent, and compliant with the aim and spirit PAIA and POPIA.

10. **OPERATOR PROVISIONS**

10.1 *WHEN THE COMPANY ENGAGES AN OPERATOR*

10.1.1 COMPLIANCE WITH POPIA

10.1.1.1 The Company recognises that when it engages third-party Operators to Process Personal Information on its behalf, such operators must comply fully with the security, confidentiality, and Processing requirements set out in POPIA.

10.1.2 DUE DILIGENCE

10.1.2.1 Before appointing any Operator, the Company will conduct a thorough due diligence assessment to evaluate the Operator's data protection capabilities, security measures, compliance history, and reputation to ensure they meet the Company's standards and POPIA obligations.

10.1.3 CONTRACTUAL OBLIGATIONS

10.1.3.1 All engagements with Operators will be governed by a written contract or data processing agreement that mandates the following:

10.1.3.1.1 Processing only as instructed: The Operator shall Process Personal Information solely on the documented instructions of the Company and not for any other purpose;

10.1.3.1.2 Security safeguards: The Operator must implement appropriate technical and organizational measures to protect Personal Information against unauthorized access, loss, destruction, or unlawful Processing;

10.1.3.1.3 Breach notification: The Operator must notify the Company immediately upon becoming aware of any data breach or security incident affecting the Personal Information;

10.1.3.1.4 Subcontracting restrictions: The Operator shall not subcontract or delegate any Processing activities without the prior written approval of the Company, and any approved subcontractors must be bound by equivalent data protection obligations; and

10.1.3.1.5 Return or destruction of data: Upon termination or expiry of the contract, the Operator must, at the Company's discretion, return all Personal Information or securely destroy it and certify such destruction.

10.1.4 ONGOING MONITORING

10.1.4.1 The Company will conduct periodic audits, assessments, or reviews of Operators to verify ongoing compliance with POPIA and PAIA, including adherence to contractual obligations and security standards.

10.2 *WHEN THE COMPANY ACTS AS AN OPERATOR*

10.2.1 PROCESSING ON INSTRUCTION

10.2.1.1 When acting as an Operator for another Responsible Party, the Company will Process Personal Information strictly in accordance with the documented instructions of that Responsible Party, without deviation or independent use.

10.2.2 CONFIDENTIALITY AND SECURITY

10.2.2.1 The Company will maintain the confidentiality and security of the Personal Information Processed and will not disclose, use, or Process the information beyond the scope agreed with the Responsible Party.

10.2.3 SECURITY SAFEGUARDS

10.2.3.1 The Company commits to implementing and maintaining the same level of technical and organizational security safeguards required under POPIA, as well as those specified in its PAIA Manual and internal POPIA compliance framework, to protect Personal Information against unauthorized access, alteration, loss, or destruction.

11. **FOREIGN INFORMATION TRANSFER**

11.1 The Company acknowledges its obligations under Chapter 9 of POPIA regarding the transfer of Personal Information outside the Republic of South Africa.

11.2 The Company will not transfer Personal Information of any Data Subject to a foreign country unless one or more of the following conditions are met, as prescribed in terms of POPIA:

11.2.1 The recipient country has laws, binding corporate rules, or binding agreements that provide an adequate level of protection substantially similar to POPIA's conditions for lawful Processing, including restrictions on further transfers;

11.2.2 The Data Subject has given explicit Consent to the transfer after being informed of the risks involved;

11.2.3 The transfer is necessary for the performance of a contract between the Data Subject and the Company, or to implement pre-contractual measures at the Data Subject's request;

11.2.4 The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a third party.

11.2.5 The transfer is for the benefit of the Data Subject, and:

11.2.5.1 It is not reasonably practicable to obtain the Data Subject's Consent; and

11.2.5.2 If it were practicable to obtain Consent, the Data Subject would likely give it.

11.3 Additional safeguards and compliance requirements implemented by the Company in respect of the transfer of Personal Information to foreign countries, includes:

11.3.1 Prior to any transfer, the Company conducts a thorough assessment of the recipient's data protection measures to ensure adequacy;

11.3.2 The Company requires third parties receiving Personal Information abroad to be bound by contractual clauses or policies that ensure compliance with POPIA's security and Processing requirements;

11.3.3 For transfers involving special Personal Information or information of children to countries without adequate protection, the Company will seek prior authorization from the Information Regulator as required by Section 57 of POPIA;

11.3.4 The Company maintains records of all cross-border transfers and related assessments for accountability and audit purposes.

12. **INFORMATION BREACH AND REPORTING TO THE INFORMATION REGULATOR**

12.1 DEFINITION OF A SECURITY COMPROMISE

12.1.1 A security compromise (commonly referred to as a data breach) occurs when there are reasonable grounds to believe that Personal Information under the control of the Company has been accessed, acquired, used, or disclosed by any unauthorized person, or has been lost, altered, or destroyed without proper authorization, in a manner that compromises the confidentiality, integrity, or availability of the information.

12.2 RESPONSIBILITIES OF THE COMPANY

12.2.1 As the Responsible Party in terms of POPIA, the Company is obligated to:

12.2.1.1 Implement appropriate and reasonable technical and organizational measures to safeguard Personal Information and prevent security compromises;

12.2.1.2 Monitor and detect any incidents or breaches affecting Personal Information; and

12.2.1.3 Respond promptly and effectively to any suspected or confirmed security compromise.

12.3 NOTIFICATION OBLIGATIONS

12.3.1 Notification to the Information Regulator

12.3.1.1 Upon discovery or reasonable suspicion of a security compromise, the Company must notify the Information Regulator as soon as reasonably possible, and where feasible, within 72 (seventy two) hours of becoming aware of the breach;

12.3.1.2 Notification must be submitted via the Information Regulator's online portal in the prescribed format;

12.3.1.3 The notification must include, at minimum:

12.3.1.3.1 A description of the nature of the breach, including categories and approximate number of affected Data Subjects and Records;

12.3.1.3.2 The name and contact details of the Company's Information Officer or CEO;

12.3.1.3.3 A description of the likely consequences of the breach;

12.3.1.3.4 Details of measures taken or planned to address and mitigate the breach; and

12.3.1.3.5 If known, the identity of the unauthorized person(s) involved.

12.3.1.4 If notification is delayed beyond 72 (seventy two) hours, the Company must provide reasons for the delay in the notification.

12.3.2 Notification to affected Data Subjects

12.3.2.1 Where a security compromise is likely to result in a high risk to the rights and freedoms of Data Subjects, the Company must notify the affected individuals without undue delay.

12.3.2.2 Notification to Data Subjects must be clear, concise, and provide sufficient information to enable them to take protective measures, including:

12.3.2.2.1 The nature and likely consequences of the breach;

12.3.2.2.2 The measures taken or planned by the Company to mitigate adverse effects;

12.3.2.2.3 Recommendations for Data Subjects to protect themselves (such as changing passwords, monitoring accounts).

12.3.2.3 Notification may be made by email, or other appropriate means, including placing a prominent notice on the Company's website if direct contact details are unavailable.

12.3.3 Exceptions to Notification

12.3.3.1 Notification to Data Subjects may be delayed if:

12.3.3.1.1 A Public Body responsible for the prevention, detection, or investigation of offences or the Information Regulator determines that notification would impede a criminal investigation; or

12.3.3.1.2 The identity of affected Data Subjects cannot be established despite reasonable efforts.

12.3.4 Operator Obligations

12.3.4.1 Operators must notify the Company immediately upon becoming aware of any suspected or actual security compromise involving Personal Information Processed on behalf of the Company.

12.3.4.2 The Company retains ultimate responsibility for reporting breaches to the Information Regulator and affected Data Subjects.

12.3.5 Internal Breach Response and Management

12.3.5.1 The Company maintains an internal data breach response plan that includes:

12.3.5.1.1 Procedures for breach identification, containment, investigation, and remediation;

12.3.5.1.2 Roles and responsibilities for breach management, including the Information Officer and senior management;

12.3.5.1.3 Documentation and record-keeping of all breaches and responses;

12.3.5.1.4 Communication protocols for internal and external stakeholders; and

12.3.5.2 Regular training and awareness programs are conducted to ensure staff understand their roles in breach prevention and response.

12.3.6 Record Keeping and Accountability

12.3.6.1 The Company keeps detailed records of all security compromises, notifications made, investigations conducted, and remedial actions taken.

12.3.6.2 These records are retained for audit and regulatory review purposes.

13. PROVISIONS RELATING TO ANY FORM OF DIRECT MARKETING BY THE COMPANY

13.1 The Company is committed to conducting direct marketing activities in compliance with POPIA and other applicable laws. This Clause 13 outlines the Company's approach to direct marketing, the rights of Data Subjects, and the procedures the Company follows to ensure lawful and responsible marketing communications.

13.2 DEFINITION OF DIRECT MARKETING

13.2.1 Direct marketing refers to the communication by any means of any advertising or marketing material directed to particular individuals to promote or offer to supply goods or services, including:

13.2.1.1 Electronic communications such as emails, SMS, WhatsApp messages, and automated calls;

13.2.1.2 Physical communications such as postal mail or printed materials;

13.2.1.3 Telephonic marketing calls.

13.3 Lawful Basis for Direct Marketing

13.3.1 The Company will only send direct marketing communications to Data Subjects where:

13.3.1.1 The Data Subject has given explicit Consent to receive such communications; or

13.3.1.2 The Company has an existing business relationship with the Data Subject, and the Data Subject has not objected to receiving direct marketing; or

13.3.1.3 The communication is made in respect of similar goods or services, and the Data Subject has been given a reasonable opportunity to object to such marketing.

13.4 CONSENT AND OPT-IN REQUIREMENTS

13.4.1 Consent for direct marketing must be voluntary, specific, and informed. The Company obtains Consent through clear opt-in mechanisms such as checkboxes on forms or explicit verbal Consent. Pre-ticked boxes or silence do not constitute valid Consent.

13.4.2 The Company maintains records of all Consents obtained for audit and compliance purposes.

13.5 RIGHT TO OBJECT AND OPT-OUT

13.5.1 Data Subjects have an unconditional right to object to the Processing of their Personal Information for direct marketing purposes at any time.

13.5.2 The Company provides clear and accessible opt-out mechanisms in all direct marketing communications, such as unsubscribe links or contact details.

13.5.3 Upon receipt of an objection or opt-out request, the Company will immediately cease sending direct marketing communications to the Data Subject.

13.5.4 The Company will ensure that opt-out requests are Processed promptly and that the Data Subject's preferences are respected in all future communications.

13.6 PROTECTION OF PERSONAL INFORMATION IN DIRECT MARKETING

13.6.1 The Company ensures that Personal Information used for direct marketing is accurate, relevant, and up to date.

13.6.2 Personal Information is Processed securely and only for the purposes Consented to by the Data Subject.

13.6.3 The Company does not share Personal Information for direct marketing purposes with third parties without explicit Consent from the Data Subject.

13.7 COMPLIANCE AND ACCOUNTABILITY

13.7.1 The Company's Information Officer oversees compliance with POPIA and PAIA requirements relating to direct marketing.

13.7.2 Employees and third-party service providers involved in direct marketing are trained on data protection obligations and the Company's policies.

13.7.3 The Company regularly reviews its direct marketing practices to ensure ongoing compliance with applicable laws and best practices.

13.8 CONTACT INFORMATION

13.8.1 Data subjects who wish to withdraw Consent, object to direct marketing, or inquire about their Personal Information may contact the Company's Information Officer.

14. **RELEVANT CONTACT DETAILS**

14.1 Information Officer:

14.1.1 Name: Pieter Johannes Swart

14.1.2 Contact number: 021 555 9000

14.1.3 Email address: Compliance@TCA.co.za

14.2 Deputy Information Officer:

14.2.1 Name: Barend Jacobus Fouche

14.2.2 Contact number: 011 620 0334

14.2.3 Email address: Compliance@TCA.co.za

14.3 Head of the Company:

14.3.1 Name: Johannes Jurie Benade

14.3.2 Contact number: 011 620 0300

14.3.3 Email address: Compliance@TCA.co.za

14.4 SAHRC:

14.4.1 Telephone: 011 877 3600

14.4.2 Email: kmonewe@sahrc.org.za

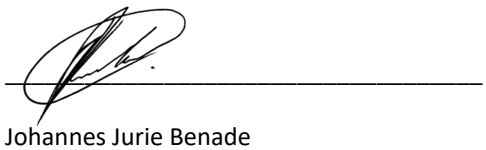
14.4.3 Website: www.sahrc.org.za

15. **PROVISION OF APPLICABLE FORMS AND DOCUMENTS**

15.1 The Company undertakes to, as far as reasonably possible, keep and make available copies of all applicable forms and documents that any Data Subject, Operator or the Company may require to complete and submit with the Information Regulator or in terms of POPIA.

16. **ADOPTION**

This PAIA Manual is formally adopted as the official PAIA manual in force and effect for the Company, by the Head of the Company in his capacity as Head of the Company on the date set out below.



Johannes Jurie Benade

Date: