THIS

POPIA INTERNAL CONTROL GUIDE

(“POPIA GUIDE")

of

Name	GMC Airconditioning Proprietary Limited
Registration Number	2023/584612/07
hereinafter “the Company”	

1. **INTERPRETATION AND DEFINITIONS**

1.1 Unless otherwise stated in this POPIA Guide:

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 POPIA Guide shall bear the same meaning throughout the entirety of this POPIA Guide;

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 POPIA Guide shall: include all genders; refer to natural persons and juristic persons; and the singular shall include the plural.

DEFINITIONS:

1.3 **Board**	refers to the Board of directors of the Company as appointed and constituted from time to time.
1.4 **Company**	refers to GMC Airconditioning Proprietary Limited with registration number: 2023/584612/07. The Company is a duly incorporated private company as envisaged in Section 8(2)(b) of the Companies Act No. 71 of 2008.
1.5 **Consent**	refers to any voluntary, specific, and informed expression of will in terms of which permission is given for the Processing of Personal Information.
1.6 **Data Subject**	refers to the individual or juristic person to whom the Personal Information relates.
1.7 **Deputy Information Officer**	refers to the person appointed to assist the Information Officer and act in their absence.
1.8 **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 serving as the liaison with the Information Regulator and Data Subjects.
1.9 **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.

1.10 **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.
1.11 **PAIA**	refers to the Promotion of Access to Information Act, 2000 including all schedules, regulations and promulgations made thereunder from time to time.
1.12 **PAIA Compliance Manual**	refers to the PAIA Compliance Manual of the Company in force and effect at any given point in time.
1.13 **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.
1.14 **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.
1.15 **POPIA Guide**	refers to the Company's internal POPIA compliance policies and/or procedures recorded in this document.
1.16 **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
1.17 **Responsible Party**	refers to the Company, as the entity that determines the purpose and means of Processing Personal Information.

2. PURPOSE AND OBJECTIVES

2.1 The purpose of this POPIA Guide is to establish a comprehensive framework for the Company to ensure compliance with POPIA and PAIA. This Guide serves as the official internal control manual that governs how Personal Information is collected, processed, stored, shared, and protected within the Company.

2.2 Key objectives of this POPIA Guide include:

2.2.1 Ensuring legal compliance: To align the Company's data Processing activities with the requirements of POPIA and PAIA, thereby avoiding legal penalties and reputational harm.

2.2.2 Protecting Data Subjects' rights: To uphold the constitutional right to privacy by safeguarding Personal Information and enabling Data Subjects to exercise their rights effectively.

2.2.3 Clarifying roles and responsibilities: To define the duties of employees, management, and appointed officers in relation to data protection.

2.2.4 Providing operational guidance: To set out practical procedures and controls for the lawful handling of Personal Information across all departments and functions.

2.2.5 Promoting a culture of privacy: To embed data protection awareness and accountability throughout the Company's operations.

2.3 This Guide applies to all employees, contractors, and third parties who handle Personal Information on behalf of the Company. It must be read in conjunction with other relevant policies such as the Company's security policies, confidentiality agreements, and the PAIA Compliance Manual.

2.4 The Guide will be reviewed annually or when legislative or operational changes occur to ensure ongoing relevance and effectiveness.

2.5 Any definition, process, procedure or otherwise not explicitly stated and/or dealt with herein shall be dealt with in accordance with the provisions of the PAIA Manual of the Company.

3. POPIA GENERAL PRINCIPLES OF LAWFUL PROCESSING OF PERSONAL INFORMATION

3.1 The Company commits to implementing and adhering to the 8 (eight) principles of lawful processing as mandated by POPIA. Each principle is explained below with the Company's intended application:

3.1.1 Accountability: The Company accepts full responsibility for ensuring compliance with POPIA. This includes:

3.1.1.1 Developing and maintaining policies, procedures, and controls to protect Personal Information;

3.1.1.2 Training employees on their data protection obligations;

3.1.1.3 Regularly monitoring and auditing compliance;

3.1.1.4 Ensuring that operators and third parties processing data on the Company's behalf also comply with POPIA through contractual agreements and oversight;

3.1.1.5 The Information Officer will be accountable for coordinating these efforts and reporting to senior management.

3.1.2 Processing Limitation: The Company will only collect and process Personal Information that is necessary and adequate for the specific purpose. It will:

3.1.2.1 Avoid excessive or irrelevant data collection;

3.1.2.2 Obtain Data Subject consent where required or rely on other lawful grounds;

3.1.2.3 Ensure that processing is lawful, fair, and not misleading to Data Subjects;

3.1.2.4 Minimize the retention period of Personal Information to what is necessary.

3.1.3 Purpose Specification: Personal information will be collected for a clear, specific, and legitimate purpose, which will be communicated to Data Subjects at the point of collection. The Company will:

3.1.3.1 Document the purposes for which data is collected;

3.1.3.2 Use the information only for those purposes unless further consent is obtained;

3.1.3.3 Avoid repurposing data without informing data subjects or obtaining new consent where required.

3.1.4 Further Processing Limitation: Any further processing of Personal Information must be compatible with the original purpose. The Company will:

3.1.4.1 Assess compatibility before any new processing activity;

3.1.4.2 Obtain new consent or ensure lawful justification if the new purpose is materially different;

3.1.4.3 Notify Data Subjects of any changes in processing activities.

3.1.5 Information Quality: The Company will take reasonable steps to ensure that Personal Information is accurate, complete, and up to date. This includes:

3.1.5.1 Regularly reviewing and updating records;

3.1.5.2 Allowing data subjects to request corrections or deletions;

3.1.5.3 Verifying information before use in decision-making or sharing.

3.1.6 Openness: The Company will be transparent about its Processing activities by:

3.1.6.1 Providing privacy notices at the point of data collection;

3.1.6.2 Making available information about the Company's data Processing policies and procedures;

3.1.6.3 Informing Data Subjects of their rights and how to exercise them.

3.1.7 Security Safeguards: The Company will implement appropriate technical and organizational security measures to protect Personal Information against unauthorized access, loss, damage, or destruction. Measures include:

3.1.7.1 Physical security controls (e.g., secure storage);

3.1.7.2 Access controls and authentication;

3.1.7.3 Encryption and secure transmission protocols;

3.1.7.4 Regular security risk assessments and audits;

3.1.7.5 Incident response and breach notification procedures.

3.1.8 Data Subject Participation: The Company will respect and facilitate Data Subjects' rights by:

3.1.8.1 Providing access to their personal information upon request;

3.1.8.2 Allowing correction or deletion requests;

3.1.8.3 Enabling objections to processing for direct marketing or other purposes;

3.1.8.4 Responding promptly and transparently to data subject requests.

4. THE COMPANY'S INFORMATION OFFICER(S)

4.1 APPOINTMENT

4.1.1 In accordance with POPIA (Sections 55 to 58), the Company will formally appoint an Information Officer and a Deputy Information Officer (if necessary). These appointments will be made by the Board or senior management and documented in writing. The appointments will be communicated internally and submitted to the Information Regulator as required.

4.2 ROLES AND RESPONSIBILITIES

4.2.1 The Information Officer is the designated individual responsible for ensuring the Company's compliance with POPIA. Their duties include:

4.2.1.1 Developing and implementing POPIA policies and procedures;

4.2.1.2 Conducting or overseeing training and awareness programs;

4.2.1.3 Monitoring the Company's processing activities and compliance status;

4.2.1.4 Acting as the primary contact point for Data Subjects and the Information Regulator;

4.2.1.5 Managing data breach responses and notifications;

4.2.1.6 Coordinating audits and risk assessments related to Personal Information.

4.2.2 The Deputy Information Officer supports the Information Officer and acts in their absence to ensure continuity of compliance efforts.

4.3 APPOINTMENT PROCESS AND DOCUMENTATION

4.3.1 The Company will establish a formal process for appointing the Information Officer and Deputy Information Officer, including criteria for suitability such as knowledge of data protection law and authority within the organisation.

4.3.2 Appointment letters will clearly outline roles, responsibilities, and reporting lines.

4.3.3 Contact details of the Information Officer and Deputy Information Officer will be made publicly available on the Company's website and internal communications.

4.4 CHANGES, REMOVAL OR RESIGNATION

4.4.1 In the event of resignation, removal, or incapacity of the Information Officer or Deputy Information Officer, the Company will promptly appoint a replacement to avoid any compliance gaps.

4.4.2 The change will be documented and communicated internally and, where necessary, notified to the Information Regulator within the prescribed timeframe.

4.4.3 Transition plans will be implemented to ensure knowledge transfer and continuity.

4.5 SUPPORT AND RESOURCES

4.5.1 The Company commits to providing the Information Officer and Deputy Information Officer with adequate resources, including:

4.5.1.1 Access to senior management support;

4.5.1.2 Budget for training, tools, and external advice if necessary;

4.5.1.3 Authority to enforce compliance measures across the organisation.

5. PERSONAL INFORMATION SAFETY MEASURES IMPLEMENTED BY THE COMPANY

5.1 The Company recognises its legal obligation under POPIA to secure the integrity and confidentiality of all Personal Information in its possession or under its control. To this end, the Company will implement appropriate, reasonable, technical, and organisational measures to prevent:

5.1.1 Loss of, damage to, or unauthorised destruction of Personal Information; and

5.1.2 Unlawful access to or Processing of Personal Information.

5.2 Technical measures include:

5.2.1 Access Controls: The Company will implement role-based access controls ensuring that only authorised personnel have access to Personal Information necessary for their duties. Multi-factor authentication will be used for accessing sensitive data systems.

5.2.2 Encryption: Personal Information stored electronically or transmitted will be encrypted using strong encryption standards to prevent interception or unauthorized access.

5.2.3 Network Security: Firewalls, intrusion detection and prevention systems, and regular vulnerability assessments will be employed to protect the Company's IT infrastructure from external and internal threats.

5.2.4 Secure Storage: Physical records containing Personal Information will be stored in locked, access-controlled environments with monitored entry.

5.2.5 Backup and Recovery: Regular backups of Personal Information will be conducted and stored securely offsite. Recovery procedures will be tested periodically to ensure data availability in case of loss.

5.2.6 Pseudonymisation and Anonymisation: Where feasible, Personal Information will be pseudonymised or anonymised to reduce exposure risks.

5.3 Organisational measures include:

5.3.1 Risk Assessments: The Company will conduct regular risk assessments to identify potential internal and external threats to Personal Information and implement safeguards accordingly.

5.3.2 Policies and Procedures: Comprehensive data protection policies will be maintained, including clear guidelines on data handling, retention, and disposal.

5.3.3 Incident Response: A formal incident response plan will be established to detect, contain, and mitigate data breaches, including timely notification to the Information Regulator and affected Data Subjects as required by POPIA.

5.3.4 Operator Management: Contracts with third-party operators will include stringent security requirements and audit rights to ensure compliance with POPIA security standards.

5.3.5 Security Awareness: Regular training and awareness programs will be conducted to ensure employees understand their responsibilities in protecting Personal Information.

5.4 The Company will continuously review and update its security measures in response to emerging threats, technological advances, and regulatory guidance, ensuring ongoing compliance and protection.

6. **STAFF TRAINING**

6.1 The Company acknowledges that human error is a significant risk to the security and lawful Processing of Personal Information. To mitigate this, the Company will provide comprehensive, ongoing training and awareness programs for all employees, contractors, and relevant third parties.

6.2 *Training Programs*

6.2.1 Induction Training: All new employees will receive mandatory POPIA training covering POPIA's principles, the Company's policies, Data Subject rights, and their individual responsibilities in handling Personal Information.

6.2.2 Role-Based Training: Specific training tailored to job functions, e.g.:

6.2.2.1 Frontline staff on lawful data collection and consent management.

6.2.2.2 IT personnel on technical safeguards and breach management.

6.2.2.3 Management on accountability and governance obligations.

6.2.3 Annual Refresher Courses: To update staff on legislative changes, emerging threats, and reinforce best practices.

6.2.4 Practical Exercises: Simulated data breach scenarios and quizzes to test understanding and preparedness.

6.2.5 Record Keeping: Training attendance and assessment results will be documented and maintained for audit purposes.

6.3 *Training Delivery Methods*

6.3.1 E-learning modules accessible remotely;

6.3.2 In-person workshops and seminars; and

6.3.3 Regular communications such as newsletters and bulletins highlighting data protection topics.

6.4 The Company will foster a culture of privacy and security awareness to ensure all personnel understand the importance of protecting Personal Information.

7. **THE COMPANY'S PAIA MANUAL**

7.1 In compliance with PAIA, the Company will maintain a comprehensive PAIA Manual which facilitates transparency and access to information.

7.2 *Paia Manual Features*

7.2.1 Accessibility: The manual will be made available on the Company's website, intranet, and in physical form at its principal place of business.

7.2.2 Content: The manual will include:

7.2.2.1 Contact details of the Company's Information Officer;

7.2.2.2 Procedures for submitting PAIA requests, including timelines and fees;

7.2.2.3 Grounds for refusal of access requests consistent with PAIA and POPIA provisions;

7.2.2.4 Description of categories of records held by the Company.

7.2.3 Alignment with POPIA: The manual will clearly explain the relationship between PAIA and POPIA, ensuring Data Subjects understand their rights to access information and how privacy is protected.

7.2.4 Review and Update: The manual will be reviewed annually or when legislative changes occur to ensure accuracy and compliance.

7.2.5 Staff Training: Employees responsible for handling PAIA requests will receive dedicated training to ensure efficient and lawful processing of requests.

8. **OPERATOR PROVISIONS**

8.1 *When the Company Engages an Operator*

8.1.1 The Company recognises that third-party operators processing personal information on its behalf must comply with POPIA's security and processing requirements.

8.1.2 Due Diligence: Before appointing an Operator, the Company will assess the Operator's data protection capabilities and reputation.

8.1.3 Contractual Obligations: Written agreements will mandate:

8.1.3.1 Processing of Personal Information only as instructed by the Company;

8.1.3.2 Implementation of appropriate security safeguards to protect Personal Information;

8.1.3.3 Immediate notification of any data breaches;

8.1.3.4 Restrictions on subcontracting without prior approval by the Company;

8.1.3.5 Obligations to return or destroy Personal Information upon contract termination.

8.1.4 Ongoing Monitoring: The Company will conduct periodic audits or reviews of Operators to verify its Operator's compliance with POPIA and PAIA.

8.2 *When the Company Acts as an Operator*

8.2.1 The Company will Process Personal Information strictly in accordance with the instructions of the responsible party.

8.2.2 It will maintain confidentiality and security of the data and will not use or disclose it beyond the agreed scope.

8.2.3 The Company will implement the same level of security safeguards as required under POPIA, the Company's PAIA Manual and this POPIA Guide.

9. **REPORTING OF A BREACH**

9.1 The Company will comply with POPIA regarding notification of security compromises involving Personal Information.

9.2 *Breach Management Process*

9.2.1 Detection and Assessment: On discovering a suspected breach, the Company will promptly investigate to determine the nature, scope, and potential impact.

9.2.2 Containment and Mitigation: Immediate steps will be taken to contain the breach and prevent further unauthorized access or damage.

9.2.3 Notification / Information Regulator: The Company will notify the Information Regulator as soon as reasonably possible, and no later than 72 (seventy two) hours after becoming aware of the breach. The notification will include:

9.2.3.1 Description of the breach.

9.2.3.2 Categories and approximate number of Data Subjects and records affected.

9.2.3.3 Measures taken or proposed to address the breach.

9.2.4 Data Subjects: If the breach is likely to result in serious harm to Data Subjects (For example identity theft, financial loss), the Company will notify affected individuals without undue delay, providing information on the nature of the breach and recommended protective actions.

9.2.5 Documentation: All breaches and responses will be documented for accountability and audit purposes.

9.2.6 Post-Incident Review: The Company will review the breach to identify root causes and implement improvements to prevent recurrence.

9.3 *Training and Testing*

9.3.1 The Company will conduct regular breach response drills to ensure preparedness.

9.3.2 Employees will be trained on their roles in breach identification and reporting.

10. **GENERAL PROVISIONS**

10.1 Review and Update: The Company undertakes to review this POPIA Guide annually and whenever there are significant changes in legislation, regulatory guidance, or business operations that affect the Processing of Personal Information. This review will ensure that this POPIA Guide remains current, effective, and aligned with evolving data protection requirements. The Information Officer is responsible for initiating and overseeing this review process.

10.2 Communication and Accessibility: The Company commits to making the latest version of this POPIA Guide readily accessible to all employees, contractors, and relevant third parties through multiple channels, including the Company intranet, email communications, and physical copies where appropriate. New employees will be introduced to this POPIA Guide as part of their onboarding process, ensuring early awareness of POPIA compliance obligations.

10.3 Accountability and Enforcement: The Company undertakes to enforce strict compliance with this POPIA Guide and POPIA across all levels of the organisation. Non-compliance with POPIA, the Company's PAIA Manual or this POPIA Guide by employees, contractors, or third parties may result in disciplinary action, which could include warnings, retraining, suspension, or termination of employment or contractual relationships. The Company will maintain records of all compliance activities, including training attendance, audits, breach reports, and remedial actions, to demonstrate accountability to the Information Regulator.

10.4 Consent and Lawful Processing: The Company commits to obtaining valid consent from Data Subjects before processing their Personal Information, except where another lawful basis under POPIA applies. The Company will maintain records of consents obtained and provide mechanisms for Data Subjects to withdraw consent at any time, in line with POPIA requirements. Consent will be:

10.4.1 Voluntary: Freely given without coercion or conditioning;

10.4.2 Informed: Provided after the Data Subject has been clearly informed about the nature, purpose, and scope of the processing; and

10.4.3 Specific and Unambiguous: Clearly indicating the Data Subject's agreement to the Processing activities.

10.5 Data Subject Rights: The Company undertakes to respect and facilitate the exercise of Data Subject rights under POPIA, including:

10.5.1 The right to access their Personal Information;

10.5.2 The right to request correction or deletion of inaccurate or outdated information;

10.5.3 The right to object to Processing for direct marketing or other specified purposes;

10.5.4 The right to be informed about the Processing of their data.

The Company will establish clear procedures to receive, process, and respond to Data Subject requests within the statutory timeframes, ensuring transparency and fairness.

10.6 Security and Breach Notification: The Company commits to maintaining robust security measures to protect Personal Information against unauthorized access, loss, or damage. In the event of a data breach, the Company will:

10.6.1 Promptly investigate and contain the breach;

10.6.2 Notify the Information Regulator within 72 (seventy two) hours of becoming aware of the breach, providing all required details as stipulated by POPIA;

10.6.3 Inform affected Data Subjects without undue delay if the breach is likely to result in serious harm;

10.6.4 Document the breach and remedial actions taken;

10.6.5 These measures align with the Information Regulator's expectations and international best practices for breach management.

10.7 Operator Management: The Company undertakes to ensure that any third-party Operators engaged to Process Personal Information on its behalf comply fully with POPIA. This includes:

10.7.1 Conducting due diligence before appointment;

10.7.2 Incorporating POPIA-compliant data protection clauses in contracts;

10.7.3 Monitoring operator compliance through audits and assessments; and

10.7.4 Ensuring Operators notify the Company immediately of any data breaches.

The Company will also adhere to its obligations when acting as an operator for other responsible parties, Processing Personal Information only as instructed and maintaining confidentiality and security.

10.8 Integration with other policies and procedures: This POPIA Guide forms part of the Company's broader governance framework and complements other relevant policies, including IT security, confidentiality, records management, and the PAIA Manual. Employees and contractors must comply with all applicable policies concurrently to ensure comprehensive data protection.

10.9 Cooperation with the Information Regulator: The Company pledges to cooperate fully with the Information Regulator in the event of investigations, audits, or compliance reviews. This includes providing requested information promptly and implementing any corrective measures recommended by the Information Regulator.

10.10 Commitment to continuous improvement: Recognising the dynamic nature of data protection, the Company commits to continuous improvement of its data protection practices. This includes staying informed of legislative developments, participating in relevant training and industry forums, and adopting new technologies and processes that enhance privacy and security.

This POPIA Guide is formally adopted by Johannes Jurie Benade (Head of the Company) on the 19th day of September 2025.

Johannes Jurie Benade