POPIA MANUAL

MCE CONSULTING ENGINEERS (PTY) LTD
t/a Moroff & Partners Consulting Engineers

(Protection of Personal Information Act, 2013 (Act No. 4 of 2013), as amended)

Registration Number: 2019/142446/07
Physical Address: 20 St James Street, Somerset West, Cape Town, 7130
Information Officer: Mr BD Le Roux
Industry: Consulting Engineering Services
Version: 1.0
Status: Tender & Compliance Ready Document
Effective Date: 2 June 2026

Table of Contents

1. INTRODUCTION

This POPIA Manual sets out the framework used by MCE Consulting Engineers (PTY) LTD to ensure lawful processing, safeguarding, and management of personal information in accordance with the Protection of Personal Information Act 4 of 2013 ("POPIA").

The organisation is committed to:

- Protecting personal information of clients, employees, suppliers, and stakeholders
- Ensuring lawful and transparent data processing
- Preventing security breaches and unauthorised access
- Upholding data subject rights

2. PURPOSE OF THIS MANUAL

The purpose of this manual is to:

- Describe how personal information is collected, processed, stored, and destroyed
- Ensure compliance with POPIA conditions
- Define roles and responsibilities for data protection
- Provide procedures for data subject rights
- Establish security and breach management controls

3. SCOPE

This manual applies to:

- All employees and contractors
- All personal information processed electronically or manually
- All clients, suppliers, subcontractors, and stakeholders
- All systems, devices, and records used by the organisation

4. KEY DEFINITIONS

- **Personal Information:** Information relating to an identifiable person
- **Data Subject:** The person to whom information relates
- **Responsible Party:** MCE Consulting Engineers (PTY) LTD
- **Operator:** Third-party processing data on behalf of the organisation
- **Processing:** Collection, storage, use, sharing, or destruction of data
- **Information Officer:** Person responsible for POPIA compliance

5. INFORMATION OFFICER & RESPONSIBILITIES

5.1 Information Officer

- Mr BD Le Roux

5.2 Responsibilities

- Ensure POPIA compliance
- Approve data processing activities
- Manage breach response
- Handle data subject requests
- Maintain security controls and policies

6. CONDITIONS FOR LAWFUL PROCESSING

Personal information is processed in accordance with POPIA Section 4 principles:

- Accountability
- Processing limitation
- Purpose specification
- Further processing limitation
- Information quality
- Openness
- Security safeguards
- Data subject participation

7. TYPES OF PERSONAL INFORMATION PROCESSED

The organisation may process:

- Identity details (names, ID numbers)
- Contact details (email, phone, address)
- Employment records
- Financial information
- Contractual and tender information
- Project and engineering documentation
- Supplier and client records

8. PURPOSE OF PROCESSING

Information is processed for:

- Engineering consulting services
- Tender submissions and contracts
- HR and employment administration
- Financial processing and billing
- Legal and regulatory compliance
- Communication with stakeholders
- Project execution and reporting

9. SHARING OF PERSONAL INFORMATION

Personal information may be shared with:

- Internal departments
- Clients and contractors (project-based only)
- Government and regulatory authorities
- Financial institutions
- Approved third-party service providers

All third parties are bound by confidentiality obligations.

10. CROSS-BORDER TRANSFER

Personal information may only be transferred outside South Africa where:

- Adequate protection laws exist, OR
- Consent is obtained, OR
- It is required for contractual purposes
- Appropriate safeguards are in place

11. SECURITY SAFEGUARDS

The organisation implements reasonable technical and organisational measures:

- Password-protected systems
- Role-based access control
- Encrypted data storage where applicable
- Secure backups
- Physical access restrictions
- Confidentiality agreements for staff
- Regular system monitoring

12. DATA SUBJECT RIGHTS

Data subjects have the right to:

- Access personal information
- Request correction or deletion
- Object to processing
- Withdraw consent (where applicable)
- Lodge complaints with the Information Regulator

13. RETENTION OF INFORMATION

Personal information is retained:

- Only as long as legally required
- For contractual and operational purposes
- According to engineering and financial regulations

Thereafter, information is securely destroyed or anonymised.

14. DATA BREACH MANAGEMENT

In the event of a security breach:

- Immediate containment is required
- Incident must be recorded
- Risk must be assessed
- Information Officer must be notified
- Affected individuals must be informed where required
- Information Regulator may be notified

Refer to:
➞ POPIA Incident Response Pack (Internal SOP)

15. DATA SUBJECT REQUEST PROCEDURE

All requests must be submitted via:

- DSAR Form (Annexure E of PAIA Manual OR internal POPIA register system, Annexure A)

Requests include:

- Access requests
- Correction requests
- Deletion requests
- Objections to processing

16. EMPLOYEE TRAINING & AWARENESS

The organisation ensures:

- POPIA awareness training

- Staff onboarding compliance briefing
- Periodic refresher training
- Data handling guidelines

17. RECORD KEEPING

Records of processing activities are maintained for:

- Audit purposes
- Legal compliance
- Tender verification
- Internal governance

18. COMPLIANCE MONITORING

Compliance is monitored through:

- Internal audits
- Incident tracking
- Access control reviews
- Annual policy review

19. APPROVAL

Approved by:

Mr BD Le Roux
Information Officer
MCE Consulting Engineers (PTY) LTD

Signature: _____

Date: _____

CONTROL INFORMATION

- Document Title: POPIA Manual
- Version: 1.0
- Classification: Confidential – Data Protection Compliance Document
- Review Cycle: Annual or legislative update
- Related Documents: PAIA Manual, Incident Response Pack

Annexure A

POPIA SOP PACK

(Standard Operating Procedures for POPIA Compliance)

MCE CONSULTING ENGINEERS (PTY) LTD

Version: 1.0
Status: Tender & Operational Compliance Document
Owner: Information Officer
Effective Date: June 2026

1. PURPOSE OF THIS SOP PACK

This SOP Pack defines the step-by-step operational procedures required to ensure compliance with the Protection of Personal Information Act (POPIA), including data handling, breach response, and data subject rights management.

It ensures:

- Consistent handling of personal information
- Legal compliance with POPIA
- Reduced risk of data breaches
- Clear accountability within the organisation

2. SOP 1: DATA BREACH RESPONSE PROCEDURE

2.1. Purpose

To ensure rapid identification, containment, and reporting of personal information breaches.

2.2. Trigger Events

- Unauthorized access to systems
- Lost or stolen devices
- Accidental email disclosure
- Malware or phishing attack
- Data corruption or system compromise

2.3. Procedure Steps

STEP 1: IDENTIFICATION

- Any employee who suspects a breach must immediately report it to:
    - Information Officer OR IT Administrator

STEP 2: IMMEDIATE CONTAINMENT (WITHIN 1 HOUR)

IT/Admin must:

- Disconnect affected systems
- Disable compromised accounts
- Reset passwords
- Block suspicious IP addresses
- Secure physical files

STEP 3: INTERNAL REPORTING (WITHIN 24 HOURS)

- Complete **Annexure C – Data Breach Form**
- Submit to Information Officer
- Log incident in Incident Register

STEP 4: RISK ASSESSMENT

Information Officer evaluates:

- Type of data exposed
- Number of data subjects affected
- Sensitivity level
- Likelihood of harm

Classification:

- Low / Medium / High / Critical

STEP 5: EXTERNAL NOTIFICATION

If required under POPIA Section 22:

- Notify Information Regulator
- Notify affected data subjects without delay

STEP 6: POST-INCIDENT ACTION

- Root cause analysis
- System patching
- Security improvement
- Staff retraining

3. SOP 2: DATA SUBJECT ACCESS REQUEST (DSAR) HANDLING

3.1. Purpose

To manage requests for access, correction, or deletion of personal information.

3.2. Procedure Steps

STEP 1: RECEIPT OF REQUEST

- Receive via email, physical form, or DSAR form (Annexure E of PAIA Manual)
- Log request in DSAR Register

STEP 2: VERIFY IDENTITY

- Request copy of ID or proof of authority
- Confirm requester is data subject or authorised representative

STEP 3: CLASSIFY REQUEST

- Access request
- Correction request
- Deletion request
- Objection to processing

STEP 4: DATA SEARCH

Relevant departments must:

- Locate all relevant records
- Ensure no unrelated personal data is included

STEP 5: INFORMATION OFFICER REVIEW

- Approve or refuse request (with legal justification if refusal)

STEP 6: RESPONSE (WITHIN REASONABLE TIME / LEGAL LIMITS)

- Provide information securely
- Or communicate refusal with reasons
- Record completion in DSAR Register

4. SOP 3: DATA CLASSIFICATION & HANDLING PROCEDURE

4.1. Purpose

To ensure personal information is properly classified and protected.

4.2. Classification Levels

Level 1: Public

- Non-sensitive company info
- Marketing material

Level 2: Internal

- Operational documents
- Internal communications

Level 3: Confidential

- Client information
- Contracts
- Project data

Level 4: Highly Confidential

- ID numbers
- Financial data
- Employee records
- Sensitive engineering project data

4.3. Handling Rules

- Level 3–4 data:
    - Must be password protected
    - Must not be shared externally without approval
    - Must be stored securely

5. SOP 4: EMAIL & INFORMATION SHARING PROCEDURE

5.1. Rules

- Verify recipient before sending sensitive data
- Use encryption or password protection where possible
- Do not send personal information to group emails unless necessary

5.2. Prohibited Actions

- Sending ID numbers without encryption
- Sharing client data via unsecured platforms
- Using personal email for company data

6. SOP 5: DATA STORAGE & RETENTION PROCEDURE

6.1. Storage Rules

- Digital data stored on secure company systems
- Physical files stored in locked cabinets
- Access restricted to authorised staff only

6.2. Retention Period

- Retain only as long as legally required
- Engineering project data retained per contractual obligations
- HR records retained per labour laws

6.3. Disposal

- Digital data: permanent deletion
- Physical files: shredding or certified destruction

7. SOP 6: THIRD-PARTY DATA SHARING PROCEDURE

7.1. Conditions

Personal information may only be shared if:

- A contract is in place
- Confidentiality agreement exists
- Processing purpose is clearly defined

7.2. Approval Process

- Request must be approved by Information Officer
- Only minimum required data must be shared

8. SOP 7: STAFF TRAINING & AWARENESS

8.1. Requirements

- All staff must undergo POPIA awareness training
- Training conducted during onboarding
- Annual refresher training required

8.2. Training Topics

- Data protection principles
- Handling personal information
- Identifying phishing attempts
- Breach reporting procedures

9. SOP 8: ACCESS CONTROL PROCEDURE

9.1. Access Principles

- Role-based access control (RBAC)
- Least privilege principle

9.2. Rules

- Employees only access data required for their job
- Access must be approved by management
- Access revoked immediately upon termination

10. SOP 9: INCIDENT LOGGING & MONITORING

10.1. Requirements

- All incidents must be recorded
- DSAR requests logged
- Breaches tracked in Incident Register

10.2. Monitoring

- Information Officer reviews logs regularly
- Identify patterns or recurring risks

11. GOVERNANCE & COMPLIANCE

- Information Officer is accountable for enforcement
- Non-compliance may result in disciplinary action
- SOPs must be reviewed annually

12. DOCUMENT CONTROL

- Version: 1.0
- Owner: Information Officer
- Review Cycle: Annual or legislative update
- Classification: Confidential – Internal Compliance Document

DOCUMENT CONTROL PAGE

1. Version History

Version	Date	Description	Author	Approved By
1.0	June 2026	Initial PAIA Manual issued	MCE Consulting Engineers	Information Officer

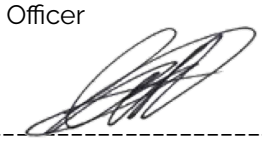
2. Review Cycle

- Next Review Date: 1 June 2027
- Review Frequency: Annual or upon legislative change

3. Approval

Approved By:

Mr BD Le Roux
Information Officer

Signature: 

Date: 2 June 2026

4. Distribution List (Optional)

This document is distributed to:

- Information Officer
- Management Team
- Compliance File
- Tender Submission Library
- External auditors (if requested)