Personal Data Protection Policy (POPIA)

FOR

MICRO DATA CENTRE CC

(Herein Referred to as MDC-IT)

MDC-IT is committed to processing data in accordance with its responsibilities under the POPI Act No. 2 of 2000 as amended ("PAIA") and Section 55 of the Protection of Personal Information

Act No. 4 of 2013 as amended ("POPI Act")

Updated: March 2021

***MDC-IT* established:**

Regulatory Risk & Compliance Management Documentation

Internal Company Policy and Procedures.

Protection of Personal Information Act (POPI Act)

https://popia.co.za/

Version	Date	Revision Author	Summary of Changes
V1	15 June 2021		POPIA Policy Created

Signed By:

…….	…….	…….	……./……/2021
(Name)	Signature)	Designation)	(Date)

1. INTRODUCTION

The Promotion of Access to Information Act 2 of 2000 (“PAIA” or “the Act”) gives effect to the constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights. The Protection of Personal Information Act 2013 has amended the PAIA and also requires from private bodies to disclose certain information through the relevant organisation’s PAIA Manual.

Specifically, section 51(1) of the Act, read with the Protection of Personal Information Act of 2013, requires a private body to compile a manual that must contain information as specified and required by both PAIA and POPI. In addition, the PAIA manual must set out the formal procedure that a person must follow in order to request to view, update or delete personal information held by the private body.

In this context, a "private body" is defined as any natural person who carries or has carried on any trade, business or profession, but only in such capacity or any partnership which carries or has carried on any trade, business or profession or any former or existing juristic person (e.g. any company, close corporation or business trust).

This organisation falls within the definition of a "private body" and this Manual has been compiled in accordance with the said provisions and to fulfil the requirements of the Act.

In terms of the Act, where a request for information is made to a body, there is an obligation to provide the information, except where the Act expressly provides that the information may not be released. In this context, Section 9 of the Act recognises that access to information can be limited. In In general the limitations relate to circumstances where such release would pose a threat to the protection of privacy, commercial confidentiality, and the exercising of efficient governance.

Accordingly, this manual provides a reference to the records held and the process that needs to be adopted to access such records.

All requests for access to information (other than information that is available to the public) must be addressed to the Head of the Business named in section 2 of this Manual.

2. BUSINESS AND CONTACT DETAILS

Name of Business: MICRO DATA CENTRE CC

Head of Business: DANIE VAN VUUREN

Position: BUSINESS OWNER

Postal Address:

Physical Address: 63 Drakensberg Ave, van Riebeeck Park, Gauteng, South Africa

Phone Number: +27 (0)10 007 5506

Email Address: danie@mdc-it.co.za

Website: www.mdc-it.co.za

3. SECTION 51(1) OF THE PROMOTION OF ACCESS TO INFORMATION ACT (THE ACT)

3.1 The Act grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

3.2 Requests in terms of the Act must be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in regulations 6 and 7 of the Act.

3.3 Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the SAHRC.

The contact details of the Commission are:

Postal Address: Private Bag 2700, Houghton, 2041

Telephone Number: (011) 877 3600

Fax Number: (011) 403 0625

Website: www.sahrc.org.za

Email: lidlamini@sahrc.org.za

4. RECORDS AVAILABLE IN TERMS OF SECTION 52(2) OF THE ACT

Not applicable.

5. RECORDS THAT ARE HELD AT THE OFFICES OF THE BUSINESS

The following is a list of records that are held at the business's office:
(see www.mdc-it.co.za/popia_act.html)

Administration

- List documents
-
-

Human Resources

- List documents
-

Operations

- List documents
-
-

Finances

- List documents
-
-

Information Technology

- List Documents
-
-

Statutory Records:

At present these include records (if any) held in terms of:

- List Records here
-
-

6. PROCESSING OF PERSONAL INFORMATION

Purpose of Processing

- List documents here
-
-

7. Personal Information processed

Natural Persons

- List documents here
-
-

Juristic Persons

- List Documents here
-
-

Categories of special information processed

- Racial / ethnic origin
-

Possible Recipients of Personal Information

- List documents

Trans-border / cross border flows of personal information

It may be required from time to time need to share personal information of data subjects with third parties in other countries. Any sharing of personal information of data subjects with third parties in other countries will be done only if the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection which effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person, as set out in the Protection of Personal Information Act and the data subject consents to the transfer.

Any such transfer will have to be shown to be necessary for the performance of a contract between the data subject and the recipient in question, or for the implementation of pre-contractual measures taken in response to the data subject's request.

General Description of Information Security Measures

Up to date technology is employed to ensure the confidentiality, integrity and availability of the Personal Information under our care.

Measures include:

- Acceptable usage of personal information
- Access control to personal information
- All third parties with whom any contract exists are required to ensure that appropriate security, privacy and confidentiality obligations are observed.
- Computer and network security including Firewalls, Virus protection software and update protocols
- Information security and HR policies including Bring Your Own Device (BYOD) policies
- Internal process to report security breach or anticipated security breach
- Investigating and reacting to security incidents.
- Logical and physical access control
- Monitoring access and usage of private information
- Physical security
- Retention and disposal of information
- Secure communications
- Training of staff members

We continuously establish and maintain appropriate, reasonable technical and organisational measures to ensure that the integrity of the Personal Information which may be in our possession or under our control, is secure and that such information is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration or access by having regard to the requirements set forth in law, in industry practice and generally accepted information security practices and procedures applicable.

8. INFORMATION REQUEST PROCEDURE

The requester must use the prescribed form to make the request for access to a record. The prescribed form is available from the Head of Business named in Section 2 above. The form is also available from the website of the Department of Justice and Constitutional Development at www.doj.gov.za

The request must be made to the Head of Business named in Section 2 above. This request must be made to the address, fax number or electronic mail address of the business.
The requester must provide sufficient detail on the request form to enable the Head of Business to identify the record and the requester. The requester should also indicate which form of access is required. The requester should also indicate if any other manner should be used to inform the requester. If this is the case, please furnish the necessary particulars to be so informed.

The requester must identify the right that is sought to be exercised or to be protected and must provide an explanation of why the requested record is required for the exercise or protection of that right.

If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of Head of Business aforesaid.

The prescribed request fee must be attached.

We will respond to your request within 30 days of receiving the request by indicating whether your request for access has been granted or denied.

Please note that the successful completion and submission of a request for access form does not automatically allow the requestor access to the requested record.

• Access will be granted to a record only if the following criteria are fulfilled:

• The record is required for the exercise or protection of any right; and

• The requestor complies with the procedural requirements set out in the Act relating to a request; and

• Access to the record is not refused in terms of any ground for refusal as contemplated in Chapter 4 of Part 3 of the Act.

8. DENIAL OF ACCESS

Access to any record may be refused under certain limited circumstances. These include:

• The protection of personal information from unreasonable disclosure concerning any natural person;

• The protection of commercial information held concerning any third party (for example trade secrets);

• The protection of financial, commercial, scientific or technical information that may harm the commercial or financial interests of any third party;

• Disclosures that would result in a breach of a duty of confidence owed to a third party;

• Disclosures that would jeopardize the safety or life of an individual;

• Disclosures that would prejudice or impair the security of property or means of transport;

• Disclosures that would prejudice or impair the protection of a person in accordance with a witness protection scheme;

• Disclosures that would prejudice or impair the protection of the safety of the public;

• Disclosures that are privileged from production in legal proceedings unless the privilege has been waived;

• Disclosures of details of any computer programme;

• Disclosures that will put Micro Data Centre at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;

• Disclosures of any record containing any trade secrets, financial, commercial, scientific, or technical information that would harm the commercial or financial interests of Micro Data Centre

• Disclosures of any record containing information about research and development being carried out or about to be carried out by Micro Data Centre

• If access to a record or any other relevant information is denied, our response will include:

• Adequate reasons for the refusal; and

• Notice that you may lodge an application with the court against the refusal and the procedure including details of the period for lodging the application.

9. FEES

The applicable fees are prescribed in terms of the Regulations promulgated under the Act.

There are two basic types of fees payable in terms of the Act.

Request Fee

The non-refundable request fee of R 50 (excluding VAT) is payable on submission of any request for access to any record. This does not apply if the request is for personal records of the requestor. No fee is payable in such circumstances.

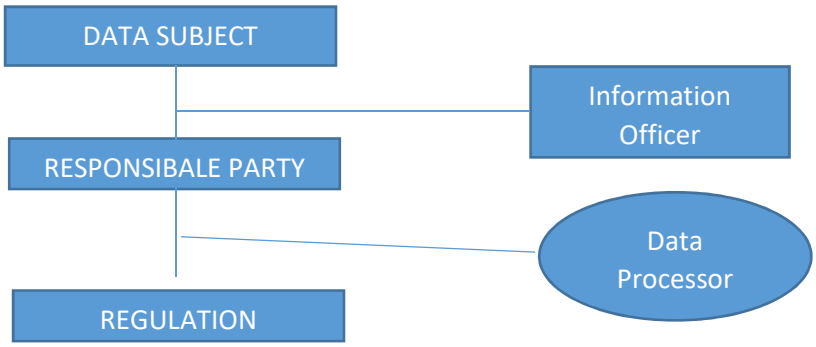
Access Fee

The access fee is payable prior to being permitted access to the records in the required form. The applicable fees are prescribed in terms of Part III of Annexure A as identified in Government Notice Number 187, Regulation 11.

10. MANUAL AVAILABILITY

A copy of this Manual may be obtained from the Head of Business referred to in Section 2 hereof
Any transmission costs or postage required in respect of hard copies of the Manual, will be for the account of the requester.

11. POPIA ROLE PLAYERS AND DEFINITIONS



11.1 DATA SUBJECT – The person who's information is being collected.

11.2 RESPONSIBLE PARTY – The organisation or person who determines the purpose or means to process the information. What is important to note there is that the Responsible Party will always remain liable. From a legal perspective the bug returns of reliability stop with the responsible party.

11.3 INFORMATION OFFICER – Is a requirement as per the POPI Act. Every Responsible Party has to appoint what is called an Information Officer. This will by default be the head of a Private Body so the CEO or the MD, but it can be delegated. Usually when you say it can be delegated to clients their eyes start to light up as the more we can move off our plate the better but what is important you can't just delegate this function to anybody in the organisation, it has to be someone of a certain level authority. The reason why we say this is that if you look at what the Information Officer is supposed to be doing it has to be someone with the ability to influence policy. His responsibility would be to assure compliance with the

POPI Act. He has to be able to influence policy and decision making around the implementation of the Act and he has to interact with the Regulator as well as receiving evaluating requests in terms of the POPI Act.

11.4 DATA PROCESSOR – This is known as a Data Processor in these days it is called an Operator. Essentially this is a third party processor. So it could be for instance a cloud provider or someone who you will appoint to your credit checks or history checks etc. What is essential is that this data processor or operator processes information on behalf of the Responsible Party the Reliable Party remains liable in the eyes of the law. As per Section 20 of the POPI Act there must be a written agreement between the Responsible Party and this third party processor, and this written agreement must then ensure and require that there are proper safeguards in place that such data processor or operator is implementing in order to process such information and that it is save. The responsibility remains with the Responsible Party and therefore it is very important that from a legal perspective that proper indemnity clauses are inserted in the agreement.

11.5 REGULATOR – The Regulators offices will be headed up by an Advocate appointed by the President of the country

11.6 MDC-IT ENGINEERING (PTY) LTD - a registered company in South Africa.

11.7 POPIA - means the General Data Protection Regulation

11.8 Register of Systems - means a register of all systems or contexts in which personal data is processed by MDC-IT

12. CONDITIONS OF LAWFULL PROCESSING

Accountability	Compliance with POPIA
Processing Limitations	Process data in a fair and lawful manner
Purpose specification	Use for explicitly defined and legitimate reasons
Use limitation	Only process further with express consent
Information Quality	Information must be reliable, accurate and up to date
Openness	Data subject must be informed of collection and grant consent for usage
Security safeguards	PI is protected against loss & unauthorised access
Individual Participation	Data subject may request information, correction and deletion- PAIA Manual

13. SCOPE AND APPLICATION OF POPIA

POPIA applies to any processing (collection, recording, organizing, sharing, using, storing etc.) of personal information by a responsible party (website, company or organization) located in South Africa or outside, if they use means to process in South Africa.

14. PROTECTION OF PERSONAL INFORMATION POLICY

Version	
Publishing Date	
Last Review Date	
Frequency of Review	Annually
Next Review Date	
Policy Owner	

15. POLICY STATEMENT

- This policy forms part of the MDC-IT's internal business processes and procedures.
- Any reference to the "organization" shall be interpreted to include the "policy owner".
- MDC-IT's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of MDC-IT are required to familiarize themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

16. APPONT A POPIA TEAM

- Appoint a project team (Legal, IT, HR etc.)
- Identify the Project Manager
- Create a Project Plan with priorities, timelines and responsible person(s)

POPI Updates	POPI Action Plan	Training Plan
• Publications by Information Regulator • Updates	• 8 Conditions • Activities under each condition	• Dates • Attendees

17. POLICY ADOPTION

By signing this document, I authorize the policy owner's approval and adoption of the processes and procedures outlined herein.

Name &	
Capacity	
Signature	
Date	

18. INTRUDUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, MDC-IT is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, MDC-IT's, employees, and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, MDC-IT is committed to effectively managing personal information in accordance with POPIA's provisions.

19. DEFINITIONS

19.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

• race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
• information relating to the education or the medical, financial, criminal or employment history of the person;
• any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
• the biometric information of the person;
• the personal opinions, views or preferences of the person;
• correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
• the views or opinions of another individual about the person;
• the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

19.2 Data Subject

Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

19.3 Responsible Party

By enlarge, the Protection of Personal Information Act, 2013 ("POPIA") only imposes obligations, duties and liabilities on the responsible party. A responsible party is defined in POPIA as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".

19.4 Operator

Section 1 of POPIA defines an operator as 'a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party'. In other words, an operator is a person (for example, a registered entity, such as a company, public authority, department, or a natural person), contracted by another person, the responsible party, to assist with the processing of personal information for such responsible party.

A simple example would be to say that an operator may be a vendor or service level provider of a company who assists MDC-IT in being able to provide its Client's with its goods or services and manage its business processing activities, such as an outsourced IT service provider, HR service provider, or a supplier to a distributing business.

19.5 Information Officer Responsibilities

The Information Officer is responsible for ensuring MDC-IT's compliance with POPIA.

Where no Information Officer is appointed, the head of MDC-IT will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
The Information Officer Registration form can be downloaded from https://www.justice.gov.za/inforeg/portal.html

19.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

• the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
• dissemination by means of transmission, distribution or making available in any other form; or
• merging, linking, as well as any restriction, degradation, erasure or destruction of information.

19.7 Record

Means any recorded information, regardless of form or medium, including:

• Writing on any material;
• Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
• Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
• Book, map, plan, graph or drawing;
• Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

19.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

19.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

19.10 De-Identify

This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

19.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

19.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

19.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

• Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
• Requesting the data subject to donate any kind for any reason.

19.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

20. POLICY PURPOSE

This purpose of this policy is to protect MDC-IT from the compliance risks associated with the protection of personal information which includes:

▪ Breaches of confidentiality. For instance, MDC-IT could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.

▪ failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose MDC-IT uses information relating to them.

▪ Reputational damage. For instance, MDC-IT could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by MDC-IT.

This policy demonstrates MDC-IT commitment to protecting the privacy rights of data subjects in the following manner:

▪ through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
▪ By cultivating an organizational culture that recognizes privacy as a valuable human right.
▪ By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
▪ By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of **MDC-IT**.
▪ By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers to protect the interests of **MDC-IT** and data subjects.
▪ By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

21. POLICY APPLICATION

This policy and its guiding principles applies to:

▪ **MDC-IT**'s governing body.
▪ **MDC-IT**' includes its affiliated, holding, subsidiary companies and branches. .
▪ All branches, business units and divisions of **MDC-IT**.
▪ All employees and volunteers.
▪ All contractors, suppliers and other persons acting on behalf of **MDC-IT**.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as **MDC-IT**'s PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).
The legal duty to comply with POPIA's provisions is activated in any situation where there is:
• A processing of.
• Personal information.
• Entered into a record.
• By or for a responsible person.
• Who is domiciled in South-Africa?

POPIA does not apply in situations where the processing of personal information:
• is concluded in the course of purely personal or household activities, or
• where the personal information has been de-identified.

22. A RIGHTS OF DATA SUBJECTS

Where appropriate, **MDC-IT** will ensure that its clients and MDC-ITs are made aware of the rights conferred upon them as data subjects. **MDC-IT** will ensure that it gives effect to the following six rights.

22.1 The Right to Access Personal Information

The Right to Access Personal Information **MDC-IT** recognises that a data subject has the right to establish whether **MDC-IT** holds personal information related to him, her or it includes the right to request access to that personal information.

22.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where **MDC-IT** is no longer authorised to retain the personal information.

22.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

In such circumstances, **MDC-IT** will give due consideration to the request and the requirements of POPIA. **MDC-IT** may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

22.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

22.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

22.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by **MDC-IT**.

The data subject also has the right to be notified in any situation where **MDC-IT** has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

23. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of **MDC-IT** will always be subject to, and act in accordance with, the following guiding principles:

23.1 Accountability

Failing to comply with POPIA could potentially damage **MDC-IT**'s reputation or expose **MDC-IT** to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

MDC-IT will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, **MDC-IT** will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

23.2 Processing Limitation

MDC-IT will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

MDC-IT will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, **MDC-IT** will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

MDC-IT will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of **MDC-IT**'s business and be provided with the reasons for doing so.

23.3 Purpose Specification

All **MDC-IT**'s business units and operations must be informed by the principle of transparency.

MDC-IT will process personal information only for specific, explicitly defined, and legitimate reasons. **MDC-IT** will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

23.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where **MDC-IT** seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary

purpose is not compatible with the original purpose, **MDC-IT** will first obtain additional consent from the data subject.

23.5 Information Quality

MDC-IT will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort **MDC-IT** will put into ensuring its accuracy.

Where personal information is collected or received from third parties, **MDC-IT** will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

23.6 Open Communication

MDC-IT will take reasonable steps to ensure that data subjects are notified (are always aware) that their personal information is being collected including the purpose for which it is being collected and processed.

MDC-IT will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether **MDC-IT** holds related personal information, or
- Request access to related personal information, or
- Request **MDC-IT** to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

23.7 Security Safeguards

MDC-IT will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

MDC-IT will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on **MDC-IT**'s IT network.

MDC-IT will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which **MDC-IT** is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

MDC-IT's operators and third-party service providers will be required to enter into service level agreements with **MDC-IT** where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in **MDC-IT**'s employment can be found under Appendix A.

23.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by **MDC-IT**. **MDC-IT** will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.
Where applicable, **MDC-IT** will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

24 INFORMATION OFFICERS

MDC-IT appointed an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.
MDC-IT's Information Officer is responsible for ensuring compliance with POPIA.
There are no legal requirements under POPIA for an organisation to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.
Where no Information Officer is available, the head of **MDC-IT** will assume the role of the Information Officer.
Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re- appointment or replacement of any Deputy Information Officers.
MDC-IT registered the Information Officer with the South African Information Regulator established under POPIA prior to performing his/her duties.

25 SPECIFIC DUTIES AND RESPONSIBILITIES

25.1 Governing Body

MDC-IT's governing body cannot delegate its accountability and is ultimately answerable for ensuring that **MDC-IT** meets its legal obligations in terms of POPIA.
The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.
The governing body is responsible for ensuring that:
• **MDC-IT**'s appointed an Information Officer, and a Deputy Information Officer if necessary.
• All persons responsible for the processing of personal information on behalf of **MDC-IT**:
• are appropriately trained and supervised to do so,
• understand that they are contractually obligated to protect the personal information they come into contact with, and
• are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
• Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
• The scheduling of a periodic POPI Audit to accurately assess and review the ways in which **MDC-IT** collects, holds, uses, shares, discloses, destroys, and processes personal information.

25.2 Information Officer

MDC-IT's Information Officer is responsible for:
• Taking steps to ensure **MDC-IT**'s reasonable compliance with the provision of POPIA.
• Keeping the governing body updated about **MDC-IT**'s information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
• Continually analysing privacy regulations and aligning them with **MDC-IT**'s personal information processing procedures. This will include reviewing **MDC-IT**'s information protection procedures and related policies.
• Ensuring that POPI Audits are scheduled and conducted on a regular basis.

• Ensuring that **MDC-IT** makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to **MDC-IT**. For instance, maintaining a “contact us” facility on **MDC-IT**’s website.
• Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by **MDC-IT**. This will include overseeing the amendment of **MDC-IT**’s employment contracts and other service level agreements.
• Encouraging compliance with the conditions required for the lawful processing of personal information.
• Ensuring that employees and other persons acting on behalf of **MDC-IT** are fully aware of the risks associated with the processing of personal information and that they remain informed about **MDC-IT**’s security controls.
• Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of **MDC-IT**.
• Addressing employees’ POPIA related questions.
• Addressing all POPIA related requests and complaints made by **MDC-IT**’s data subjects.
• Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, regarding any other matter.
• The Deputy Information Officer will assist the Information Officer in performing its duties.

25.3 IT Manager (may be part of Information Officer’s responsibilities)

MDC-IT’s IT Manager is responsible for:
• Ensuring that **MDC-IT**’s IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
• Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
• Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
• Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
• Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
• Ensuring that personal information being transferred electronically is encrypted.
• Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
• Performing regular IT audits to ensure that the security of **MDC-IT**’s hardware and software systems are functioning properly.
• Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
• Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on **MDC-IT**’s behalf. For instance, cloud computing services.

25.4 Marketing & Communication Manager (may be part of Information Officer’s responsibilities)

MDC-IT’s Marketing & Communication Manager is responsible for:
• Approving and maintaining the protection of personal information statements and disclaimers that are displayed on **MDC-IT**’s website, including those attached to communications such as emails and electronic newsletters.

• Addressing any personal information protection queries from journalists or media outlets such as newspapers.
• Where necessary, working with persons acting on behalf of **MDC-IT** to ensure that any outsourced marketing initiatives comply with POPIA.

25.5 Employees and other Persons acting on behalf of MDC-IT

Employees and other persons acting on behalf of **MDC-IT** will, during the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers, and other employees.

Employees and other persons acting on behalf of **MDC-IT** are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of **MDC-IT** may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within **MDC-IT** or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties. Employees and other persons acting on behalf of **MDC-IT** must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of **MDC-IT** will only process personal information where:
• The data subject, or a competent person where the data subject is a child, consents to the processing; or
• The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
• The processing complies with an obligation imposed by law on the responsible party; or
• The processing protects a legitimate interest of the data subject; or
• The processing is necessary for pursuing the legitimate interests of **MDC-IT** or of a third party to whom the information is supplied.
• Furthermore, personal information will only be processed where the data subject:
• Clearly understands why and for what purpose his, her or its personal information is being collected; and
• Has granted **MDC-IT** with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of **MDC-IT** will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, **MDC-IT** will keep a voice

recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
• the personal information has been made public, or
• where valid consent has been given to a third party, or
• the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of **MDC-IT** will under no circumstances:
• Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
• Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from **MDC-IT**'s central database or a dedicated server.
• Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
• Transfer personal information outside of South Africa without the express permission from the Information Officer. Employees and other persons acting on behalf of **MDC-IT** are responsible for:
• Keeping all personal information that they encounter secure, by taking sensible precautions and following the guidelines outlined within this policy.
• Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
• Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of **MDC-IT**, with the sending or sharing of personal information to or with authorised external persons.
• Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
• Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
• Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
• Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
• Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
• Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or MDC-IT phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
• Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where

personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
• Undergoing POPI Awareness training from time to time.
• Where an employee, or a person acting on behalf of **MDC-IT**, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy

26 POPI AUDIT

MDC-IT's Information Officer will schedule periodic POPI Audits. The purpose of a POPI audit is to:
• Identify the processes used to collect, record, store, disseminate and destroy personal information.
• Determine the flow of personal information throughout **MDC-IT**. For instance, **MDC-IT**'s various business units, divisions, branches, and other associated organisations.
• Redefine the purpose for gathering and processing personal information.
• Ensure that the processing parameters are still adequately limited.
• Ensure that new data subjects are made aware of the processing of their personal information.
• Re-establish the rationale for any further processing where information is received via a third party.
• Verify the quality and security of personal information.
• Monitor the extend of compliance with POPIA and this policy.
• Monitor the effectiveness of internal controls established to manage **MDC-IT**'s POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with line managers to identify areas within in **MDC-IT**'s operation that are most vulnerable or susceptible to the unlawful processing of personal information.
Information Officers will be permitted direct access to and have demonstrable support from line managers and **MDC-IT**'s governing body in performing their duties.

27 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:
• Request what personal information **MDC-IT** holds about them and why.
• Request access to their personal information.
• Be informed how to keep their personal information up to date.
Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against **MDC-IT**'s PAIA Policy.

The Information Officer will process all requests within a reasonable time.

28 POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. **MDC-IT** takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

• POPI complaints must be submitted to **MDC-IT** in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".

• Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.

• The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

• The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.

• The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on **MDC-IT**'s data subjects.

• Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with **MDC-IT**'s governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

• The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to **MDC-IT**'s governing body within 7 working days of receipt of the complaint. In all instances, **MDC-IT** will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

• The Information Officer's response to the data subject may comprise any of the following:

• A suggested remedy for the complaint,

• A dismissal of the complaint and the reasons as to why it was dismissed,

• An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

• Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

• The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

29 DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, **MDC-IT** may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, **MDC-IT** will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which **MDC-IT** may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets to limit any prejudice or damages caused.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address:	

Please be aware that we may require you to provide proof of identification prior to processing your request.

There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Request	
I request **MDC-IT**' to:	
(a) Inform me whether it holds any of my personal information	
(b) Provide me with a record or description of my personal information	
(c) Correct or update my personal information	
(d) Destroy or delete a record of my personal information	

C. Instructions

D. Signature Page
Signature
Date

ANNEXURE B: POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer:	
Name	
Contact Number	
Email Address:	

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator.

The Information Regulator: Ms Mmamoroke Mphelo

Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria

Email: inforreg@justice.gov.za

Website: http://www.justice.gov.za/inforeg/index.html

A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature:	
Date	

ANNEXURE G

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

(ACT NO.4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017

[Regulation 2(1)]

Note:

1. *Affidavits or other documentary evidence in support of the objection must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

Reference Number……..

A	**DETAILS OF DATA SUBJECT**
Name and surname of data subject: Residential, postal or business address:	
Contact number(s):	
Fax No:	
Contact No:	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name and surname of responsible party(if the responsible party is a natural):	
Residential, postal or business address:	
Contact number(s):	
Fax number:	
E-mail address:	
Name of public or private body(if the responsible party is not a natural person):	

Business address:	
Contact number(s):	
Fax number:	
E-mail address:	
C	**REASONS FOR OBJECTION** (Please provide detailed reasons for the objection)