POPIA, PAIA & FIC 8

POLICY & MANUAL

This Policy applies to **FIBRE4BUSINESS (SP)**

(the “Company”)
(Including all Subsidiaries & Associations)

Registered office address:

1604 Horizon Bay
2 Blaauwberg Road
Table View
7441

Contact Details: **Telephone: 082 373 2811**
Email: mikaelmendonca@gmail.com

THIS POLICY WAS PREPARED BY MJSC (PTY) LTD,

© MJSC (Pty) Ltd

IN ACCORDANCE WITH THE
POPIA NO 4 OF 2013, PAIA NO 2 OF 2000 & FIC DIRECTIVE 8 OF 2023

Contents

1. DEFINITIONS 3
2. INTRODUCTION 4
3. DETAILS OF INFORMATION OFFICER 6
4. THE ACT 8
5. SCOPE 8
6. CODE OF CONDUCT 9
7. POLICY WITH REGARD TO CONFIDENTIALITY AND ACCESS TO INFORMATION 9
8. RECORDS AUTOMATICALLY AVAILABLE 10
9. RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION: 10
10. PARTICULARS IN TERMS OF SECTION 51 OF THE PAIA 10
11. GUIDE ON HOW TO USE THE PAIA 11
12. SUBJECTS AND CATEGORIES OF RECORDS HELD BY THE COMPANY 12
13. RECORDS THAT ARE NOT AUTOMATICALLY AVAILABLE 13
14. REQUEST PROCEDURE 13
15. FEES 15
16. THIRD PARTIES 15
17. GROUNDS FOR REFUSAL ACCESS TO RECORDS IN TERMS OF SECTION 62-69 OF THE ACT 16
18. APPEAL - REMEDIES 17
19. PROHIBITIONS OF SPECIAL PERSONAL INFORMATION 18
20. DESTRUCTION OF INFORMATION 18

© MJSC (Pty) Ltd

1. DEFINITIONS

"**Code of Conduct**" refers to a code of conduct issued under Chapter 7 of the Act.

"**Consent**" refers to any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of information.

"**Data Subject**" refer to a person to whom personal information relates.

"**De-identify**" refers to personal information of a data subject, means to delete information that-

(a) identifies the data subject.
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; and
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

"**FIC Directive 8**" refers to the screening of employees for competence and integrity with scrutinizing of employees against applicable sanctions lists as a money laundering, terrorist financing and proliferation financing control measure.

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

"**Information Officer**" refers the head of a private body as contemplated in Sect 1 of the PAIA.

"**Operator**" refers to a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party.

"**Person**" refers to a natural person or a juristic person.

"**Personal Information**" refers to information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including but not limited to –

(a) Info relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.
(b) Info relating to education or medical, financial, criminal or employment history of a person.
(c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to a person.
(d) Biometric information of a person.
(e) Personal opinion, views or preferences of a person.
(f) Views of another person about a person

"**Processing**" refers to any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

© MJSC (Pty) Ltd

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

"**Record**" refers to recorded information regardless of the form or medium, including written material, information produced (software) or devices or stored information.

2. INTRODUCTION

The **Promotion of Access to Information Act, 2000** (the "PAIA Act") provides 3rd parties the right to approach private bodies and the government to request information held by them, which is required in the exercise and/or protection of any rights.

The **Protection of Personal Information Act, 2013** (the "POPI Act") provides for the lawful procession of Personal Information by or for a responsible party as follow:

2.1. Accountability

The responsible party must ensure that conditions for lawful processing is implemented and controlled in terms of the purpose of such information and appointed accountability.

2.2. Processing Limitations

Personal Information must be processed in a lawful manner and in a reasonable manner that does not infringe on the privacy of the data subject.

Such processing of information may only be done if given the purpose for which it is intended to be processed, it is adequate, relevant and not excessive.

Processing of information may only be done where such processing is required for:

2.2.1. contractual obligations;
2.2.2. out of actions for conclusion or performance of a contract term to which the data subject is party to;
2.2.3. respective law / legislation;
2.2.4. protects the legitimate interest of the data subject;
2.2.5. necessary for the proper performance of a public law duty by a public body; and
2.2.6. pursuing the legitimate interest of a responsible party or 3rd party to whom the information is supplied.

Personal Information may only be collected directly from the data subject unless so derived from a public record or deliberately made public by the data subject.

The **FIC Directive 8** (the "FIC 8") provides and requires any business that deals with internal financial matters and that of creditors or debtors to undertake annual risk assessments on the personal and / or service providers that deals with the financial affairs of the business or clients. The directive has been issued in terms of the Financial Intelligence Centre Act (No 38 of 2001) to which every business will be held accountable.

© MJSC (Pty) Ltd

2.3. Purpose specification

The Company must ensure that explicit reasoning and amendment of all source documentation is implemented in order to obtain the required permissions from all data subjects in terms of collection, processing and record keeping purposes.

Data retention may not exceed the legislative indications such as Financial Information, 10 years and Personnel Information 5 years.

Such permissions to retain information as per legislation or longer, must be in writing and explicitly agreed to by the data subject.

Destroying of information must be done in a controlled manner as to ensure that such destruction is legal and fully compliant with the knowledge of the data subject.

The purpose for the FIC 8 inclusion outlines the accountability of institutions and / or individuals that works directly with financial matters, money and banking information. It is imperative that each person and business within these areas are duly screened and assessed for competence and integrity. Such access to information of a financial matter must be listed, assessed, monitored, mitigated and managed against risks against money laundering, terrorist financing and proliferation financing.

2.4. Information Quality

A reasonable person must take reasonable steps to ensure that information is accurate, up to date, not misleading or false, and completed.

2.5. Openness

The company must ensure that the data subject is well aware of the following:

2.5.1. What information is being collected, for what reason and where such information will be stored or processed;
2.5.2. Name and address of responsible person;
2.5.3. Purpose of collection;
2.5.4. Mandatory and voluntary information collection;
2.5.5. Consequences for failing to provide correct and accurate information;
2.5.6. What transfer is intended to be transferred or utilized in terms of contractual obligations and with which 3rd party;
2.5.7. Any objection by the data subject submission in storing or processing of any information.

2.6. Security safeguard

The Company must ensure that the integrity and confidentiality of all data subject information in its possession or under its control is maintained at all times by taking appropriate, reasonable, technical and organisational measures to prevent loss, damage or unlawful usage of such information.

© MJSC (Pty) Ltd

The company must ensure that a comprehensive agreement between consultants and / or service providers entrusted with such processing of personal information is undersigned with limitations and restrictions as per the Act on such Businesses.

Regular audits and confirmations are to be implemented to ensure full compliance on an annual basis.

All accountable individuals and institutions must provide information and sureties in terms of FIC 8 compliance in that a periodic risk-based assessment is conducted with vetting of staff.

2.7. Data subject participation

A data subject, where adequate proof of identification has been provided, may request a responsible party to confirm whether or not a reasonable party holds personal information about the data subject. Any such records may be requested with instruction to destroy and / or maintain control over such information.

Where such information or confirmation of stored information is requested, the responsible party / person / company will have 30 days to confirm and / or supply such information.
A data subject may be requested to confirm current and / or active information with the responsible person annually and / or request to have amendments / changes made to such information in order to update and / or amend information from time to time.

Constitution of the Republic of South Africa, 1996 section 14, provides that everyone has the right to privacy. The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

The POPI Act gives a Data Subjects the right to, in the prescribed manner, request a Responsible Party to correct, amend, change or delete Personal Information about the Data Subject in its possession or under its management and control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. Such information may be requested to be destroy or to delete a record of Personal Information about the Data Subject that the Responsible Party is no longer authorised to retain access and/or request the correction or deletion of any Personal Information held about them that may be inaccurate, misleading or outdated.

The Company endorses and complies with the PAIA Act and POPI Act and believes that this Policy will assist all in exercising their rights and obligations. The Act seeks, *inter alia*, to give effect to the constitutional right of access to any information held by the state or by any other person where such information is required for the exercise or protection of any right.

3. DETAILS OF INFORMATION OFFICER

The Information Officer of the Company is referred to as the head of a private body or an identified or appointment Information Officer who is responsible for and accountable for all matters pertaining to the Acts and this Policy.

© MJSC (Pty) Ltd

The Company hereto note that the following identified, trained and orientated individual are appointed in terms of the Information Officer:

Name:	Mikael Mendonca
Physical Address:	1604 Horizon Bay 2 Blaauwberg Road Table View 7441 Republic of South Africa
Telephone Number:	+27(0) 82 373 2811
E-mail:	mikaelmendonca@gmail.com

The Company hereto confirms that in terms of FIC 8, the following accountable person is and will be responsible for all Risk-based assessments, recording and monitoring:

Name:	Mikael Mendonca
Physical Address:	1604 Horizon Bay 2 Blaauwberg Road Table View 7441 Republic of South Africa

3.1. **Duties and Responsibilities of an Information Officer**

The appointment of an Information Officer is made by the Company Shareholders / Management and / or Owner in terms of the law. Where so deemed necessary a Deputy Information Offer may be appointed at the discretion of the Company.

The responsibilities include:

3.1.1. Ensuring the Companies / Organizations compliance with the provision of POPIA.
3.1.2. Keeping the governing body updated on all the organizations information protection responsibilities under POPIA.
3.1.3. Constantly reviewing the privacy regulations and aligning the organizations personal information processing procedures
3.1.4. Ensuring that POPI Audits are scheduled and conducted on a regular basis.
3.1.5. Ensuring a convenient way for data subjects to update their personal information and submit complaints to the organization.
3.1.6. Approving of contracts entered into with operators, employees and other third parties, which may have an impact on the personal information held by an organization.
3.1.7. Ensuring compliance with the conditions required for the lawful processing of personal information.
3.1.8. Ensuring that employees and other persons acting on behalf of the organization are fully aware of the risks associated with the processing of personal information, and that they remain informed of the company's security controls.

© MJSC (Pty) Ltd

3.1.9. Induction training of awareness training of employees and other individuals involved in the processing of the personal information on behalf of the company.
3.1.10. Addressing the employees POPIA related questions
3.1.11. Addressing all POPIA related requests and complaints made by the organizations data subjects.
3.1.12. Working with the Information Regulator in relation to any ongoing investigations. Acting as the contact point for the Information Regulator Authority on issues, relating to the processing of personal information and to consult where appropriate.

3.2. **Duties and Responsibilities of an FIC 8 Risk Officer**

The appointment of a Risk Officer can be associated with a position such as Financial Officer and / or Internal Control. The Company Shareholders will be required to identify the best level of staff member in order to make such appointment.

The duties of the risk officer can be outlined and inclusive of the following:

3.2.1. Compile and record the risk-based factors that are identified within the business.
3.2.2. Identify the respective positions and individuals as per the structure of the Company in order to conduct the respective orientation, verifications and contractual obligations.
3.2.3. Ensure that all risk-based assessments are outlined, recorded and safeguarded for reporting and future reference.
3.2.4. Ensure that the respective vetting is conducted annually and recorded.
3.2.5. Outline steps to be taken where vetting has failed and / or where a breach has occurred or been identified.
3.2.6. Create measures that will mitigate breaches and how it will be recorded, handled and eliminated.
3.2.7. Ensure that all staff and the institution is protected against any breaches of FIC 8.

4. THE ACT

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.

Requests in terms of the ACT shall be made in accordance with the prescribed procedures, at the rates provided.

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.

5. SCOPE

This Policy has been prepared in respect of the Company or Group of Companies, which includes the following related entities:

© MJSC (Pty) Ltd

- ✓ Assessing your company requirements for Optic Fibre and ISP products to meet your business connectivity needs.
- ✓ Matching feasible ISP products to your company requirements.
- ✓ Finding applicable Fibre Optic Providers at your Business location. These include Cybersmart (Lightspeed Fibre), Vumatel, Frogfoot, Dark Fibre Africa, Openserve
- ✓ Providing best fit ISP products and pricing.
- ✓ Managing the application process, installation timelines and activation of your ISP product with Cybersmart internally.
- ✓ Obtaining technical support from Cybersmart for any specific technical requirements as needed
- ✓ Liaising with your current IT support teams regarding setup and internal networking requirements.
- ✓ Offer 3rd party recommendations for both Internal IT requirements (Desk top support) and Internal Networking setup (WIFI, Ethernet and VOIP).
- ✓ Offer ongoing Aftersales queries and technical inputs as needed.

The scope of this Policy excludes the Company's operations outside the Republic of South Africa and will serve to provide a reference regarding the records held by the Company at its Registered Office and various operations within the borders of the Republic of South Africa.

6. CODE OF CONDUCT

It is advisable that every person responsible for maintaining control and safeguarding, processing and managing of personal information be issued with a code of conduct that is required to be undersigned and duly followed, in terms of the following:

6.1. Conditions under which the lawful processing of personal information may be conducted.
6.2. Conditions setting out the functional equivalent of all the obligations of such conditions.
6.3. Description of how lawful actions must be conducted.
6.4. Specify measures to be taken in storing data, disposing of data, manage requested data, legislative indications on data, etc.

The Company is required to set up complaint channels and procedures in terms of this Policy. Clear terms and timelines must be communicated in terms of managing complaints with record keeping.

7. POLICY WITH REGARD TO CONFIDENTIALITY AND ACCESS TO INFORMATION

The Company will protect the confidentiality of information provided to it by a data subject or 3rd parties, subject to the Company's obligations to disclose information in terms of any applicable law or regulation or a court order requiring disclosure of information. If access is requested to a record that contains information about a 3rd party, the Company is obliged to attempt to contact such 3rd party or data subject to inform them of the request.

© MJSC (Pty) Ltd

The Company will give the party an opportunity of responding by either consenting to the access or by providing reasons why the access should be denied. In the event that the party furnishing reasons for the support or denial of access, the Information Officer will consider these reasons in determining whether access should be granted to the requestor or not.

8. RECORDS AUTOMATICALLY AVAILABLE

The categories of records that are automatically available without a person having to request access in terms of the PAIA Act [Section 51(1)(c)].

- ✓ Records of the Company lodged in terms of government requirements such as the Registrar of Deeds.
- ✓ Documentation and information relating to the Company which is held by the Companies and Intellectual Properties Commission in accordance with the requirements set out in set out in section 25 of the Companies Act 71 of 2008;
- ✓ Product and Services Brochures; and
- ✓ News and other Marketing Information.

Certain other information relating to the Company's is also made available on said website from time to time, which is deemed public record.

9. RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION:

Records are kept in accordance with such other legislation as applicable to the Company, which includes, but is not limited to:

No	Reference	Act
1	No 61 of 1973	Companies Act
2	No 98 of 1978	Copyright Act
3	No 55 of 1998	Employment Equity Act
4	No 95 of 1967	Income Tax Act
5	No 66 of 1995	Labour Relations Act
6	No 89 of 1991	Value Added Tax Act
7	No 37 of 2002	Financial Advisory and Intermediary Services Act
8	No 75 of 1997	Basic Conditions of Employment Act
9	No 69 of 1984	Close Corporations Act
10	No 25 of 2002	Electronic Communications and Transactions Act
11	No 02 of 2000	Promotion of Access of Information Act
12	No 30 of 1996	Unemployment Insurance Act
13	No 38 of 2001	Financial Intelligence Centre Act

10. PARTICULARS IN TERMS OF SECTION 51 OF THE PAIA

10.1. The PAIA Act seeks to advance a culture of transparency and accountability in both public and private bodies. The legislation was enacted as a direct response to Section 32(2) of the Constitution of South Africa (the right of access to information) which requires

© MJSC (Pty) Ltd

that the Government implements laws in an effort to make information pertaining to public and private bodies more accessible to all.

10.2. 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. Where a request is made in terms of the PAIA Act, the body to whom the request is made is obliged to release the information, except where the PAIA Act expressly provides that the information may or must not be released.

10.3. One of the main requirements specified in the PAIA Act is the compilation of a Policy that provides information on both the types and categories of records held by the public or private body. In terms of the PAIA Act, the Company is regarded as a “private body” and therefore the requirements regarding access must follow the provisions of the PAIA Act relevant to private bodies and more in particular Section 51 of the PAIA Act.

10.4. In compliance with Section 51 of the PAIA Act this PAIA Policy sets out the following details:

10.4.1. The Company’s contact details including, physical and postal addresses, telephone and fax numbers, electronic mail address of the person tasked in terms of this Code of Conduct;
10.4.2. Information on how to obtain and access this Code of Conduct and a guide on how to use it;
10.4.3. Categories of information held by the Company that is available without a person having to formally request such details in terms of the PAIA Act;
10.4.4. Categories of information held by the Company that is available in accordance with other legislation and which, subject to the PAIA Act, may be made available by the Company on receipt of and consideration of a formal request, made in terms of the PAIA Act;
10.4.5. Sufficient information to facilitate a request for access to records and a description of the subjects on which records are available from the Company;

10.5. Adherence to these requirements entails not only compilation of the external Policy but also compliance with the general provisions stated in the PAIA Act.

11. GUIDE ON HOW TO USE THE PAIA

11.1. The Human Rights Commission has been tasked with the administration of the PAIA Act.

11.2. In terms of Section 10 of the PAIA Act, the Human Rights Commission has compiled a guide which is intended to assist users in the interpretation of the PAIA Act and how to access the records of private and public bodies and the remedies available in law regarding a breach of any of the provisions of the PAIA Act.

11.3. Should any person have queries or concerns relating to their rights and in particular their right to access information from a private or public body, such queries should be directed to:

© MJSC (Pty) Ltd

The South African Human Rights Commission PAIA Unit
Private Bag X2700
Houghton, 2041
Republic of South Africa

Business phone: +27 11 877 3600
Fax: +27 11 403 0625
Email address: section51.paia@sahrc.org.za
Website: www.sahrc.org.za

12. SUBJECTS AND CATEGORIES OF RECORDS HELD BY THE COMPANY

The list below depicts records of information which the Company has available in terms of laws applicable to the Company:

12.1. Corporate Secretariat and Governance

- ✓ Applicable Statutory Documents
- ✓ Policies and Procedures
- ✓ Code of Conduct
- ✓ Records relating to the appointment of directors and auditor
- ✓ Health & Safety Records
- ✓ Share Certificates
- ✓ Legal Compliance Records
- ✓ Share Register and other statutory registers
- ✓ Memoranda of Incorporation
- ✓ Statutory Returns to Relevant Authorities

12.2. Finance and Taxation

- ✓ Accounting Records (including Ledgers and Reconciliations)
- ✓ Annual Financial Statements
- ✓ Audit Report (where applicable)
- ✓ Client information in terms of a Service Level Agreement
- ✓ Bank Records and Statements
- ✓ SARS records (PAYE, UIF and SDL)
- ✓ SARS records of employees (IRP5's)
- ✓ Debtors and Creditors statements and invoices
- ✓ Income Tax numbers of Staff
- ✓ VAT numbers of clients
- ✓ Workmen's Compensation Returns and LOGS

12.3. Personal Documents and Records

- ✓ CV's, application forms and personal details of any applicant
- ✓ Personal information including ID's, Criminal Checks, References, Banking details
- ✓ Disciplinary Code and Records
- ✓ Leave Records
- ✓ Job Profiles
- ✓ Letters of Appointment and Contracts
- ✓ Dispute resolution records

© MJSC (Pty) Ltd

- ✓ Organisational Structures
- ✓ Employment Equity information
- ✓ Termination Documentation
- ✓ Qualifications
- ✓ Payroll reports and information
- ✓ Employee Benefit forms and information (3rd party requirements)

12.4. **Intellectual Property**

- ✓ Intellectual property pertaining to solutions and
- ✓ Know-how products developed

12.5. **Corporate Affairs and Investor Relations / Communications**

- ✓ Media Releases
- ✓ Newsletters and Publications

12.6. **Legal**

- ✓ Agreements and Contracts
- ✓ Health and Safety Records
- ✓ Client disputes and client employee disputes

12.7. **Sales, Marketing and Communications**

1. Actual Sales
2. Branding
3. Press releases / communique
4. External Publications
5. Media and advertising
6. Proposals and Tenders

13. RECORDS THAT ARE NOT AUTOMATICALLY AVAILABLE

Records of the Company which are not automatically available must be requested in terms of the procedure set out in this Policy and which may be subject to the restrictions and right of refusal to access as provided for in the Act.

14. REQUEST PROCEDURE

14.1. The Company is mainly concerned about protecting the confidential information of its Data Subjects at all times.

14.2. Any person making a request for access to records of the Company is referred to as a “requester”. The requester must comply with all the procedural requirements contained in the PAIA Act relating to the request for access to records.

14.3. The requester must complete the prescribed form application form attached hereto as **Form C** and submit the form, to the Information Officer of the Company at the postal or physical, fax or electronic mail address as stated above.

14.4. The prescribed form must be filled in with sufficient particulars to at least enable the Information Officer of the Company to identify:

© MJSC (Pty) Ltd

14.4.1. record or records requested;
14.4.2. identity of the requester;
14.4.3. which form of access is required if the request is granted; and
14.4.4. postal address, telephone number and fax number of the requester.

14.5. The requester must state that he/she requires the information to exercise or protect her/his right and clearly state what the nature of the right is to be exercised or protected. In addition, the requester must clearly specify why the records are necessary to exercise or protect such a right.

14.6. Such request must be processed within 30 (thirty) days after the request has been received.

14.7. The requester shall be informed whether the access has been granted or denied within 30 (thirty) days of receipt of the request and give notice with reasons to that effect.

14.8. The 30 (thirty) day period within which the Company must decide whether to grant or refuse the request, may be extended for a further period of not more than 30 (thirty) days if the request is for a vast amount of information, or the information cannot reasonably be obtained within the original 30 (thirty) day period. The Information Officer will notify the requester in writing should an extension be sought.

14.9. If the request for access is granted, the Deputy Information Officer of the Company must advise the requestor:

14.9.1. the access fee (if any) to be paid upon access;
14.9.2. the form in which access will be given; and
14.9.3. that the requester may lodge an application with a court against the access fee to be paid or the form of access granted, and the procedure, including the period allowed, for lodging the application.

14.10. If the request for access is refused, the Information Officer of the Company must:

14.10.1. state adequate reasons for the refusal, including the provisions of this Act relied on;
14.10.2. exclude, from any such reasons, any reference to the content of the record; and
14.10.3. state that the requester may lodge an application with a court against the refusal of the request, and the procedure (including the period) for lodging the application.

14.11. In terms of Section 54 of the PAIA Act, if all reasonable steps have been taken to find the record requested and there are reasonable grounds to believe that the record is in possession of the Company but cannot be found, and if it does not exist, then the Information Officer of the Company must notify by way of affidavit or affirmation, the requester that it is not possible to give access to that record.

© MJSC (Pty) Ltd

14.12. If after notice is given, the record in question is found, the requester must be given access thereto unless the ground for the refusal of access exists.

14.13. If the request is declined for any reason the notice must include adequate reasons for the decision, together with the relevant provisions of the PAIA Act relied upon and provide the procedure to be followed should the requester wish appeal the decision.

14.14. Section 59 provides that the Information Officer of the Company may serve a record and grant access only to that portion which the law does not prohibit access to.

15. FEES

15.1. The Act provides for two types of fees, namely:

15.1.1. A request fee, which will be a standard fee; and

15.1.2. An access fee, which must be calculated by considering reproduction costs, search and preparation time and costs, as well as postal costs.

15.2. When the request is received by the Information Officer of the Company, such person shall by notice require the requester to pay the prescribed request fee, if any, before further processing of the request.

15.3. If a requester requires access to records of his/her Personal Information, there shall be no request fee payable. However, the requester must pay the prescribed access and reproduction fees for such Personal Information.

15.4. If the search for the record has been made and the preparation of the record for disclosure including arrangements to make it available in the request form, requires more than the hours prescribed in the regulations for this purpose, the Deputy Information Officer of the Company shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.

15.5. The Information Officer of the Company shall withhold the record until the requester has paid the fees as indicated hereto.

15.6. A requester whose request for access to a record has been granted, must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the records for disclosure including making arrangements to make it available in the request form.

15.7. If a deposit has been paid in respect of a request for access, which is refused, then the Deputy Information Officer of the Company must repay the deposit to the requester with interest at the prescribed rate.

16. THIRD PARTIES

16.1. If the request is for the record pertaining to the third party, the Information Officer of the Company must take all reasonable steps to inform the third party of the request. This must be done within 21 (twenty-one) days of receipt of the request. The way this is done must be by the fastest means reasonably possible, but if orally, the Information Officer of the Company must thereafter give the third party a written confirmation of the notification.

© MJSC (Pty) Ltd

16.2. The third party may within 21 (twenty-one) days thereafter either make representation to the Company as to why the request should be refused; alternatively grant written consent to the disclosure of the record.

16.3. The third party must be advised of the decision taken by the Information Officer of the Company whether to grant or to decline the request. A third party who is dissatisfied with the Information Officer of the Company's decision to grant a request for information, may within 30 (thirty) days of notification of the decision, apply to a Court for relief.

17. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF SECTION 62-69 OF THE ACT

The Company has the right to refuse access to information on one or more of the following grounds:

17.1. ***Mandatory protection of the privacy of a third*** party ***who is a natural person***, if such disclosure would involve the unreasonable disclosure of Personal Information about a third party, including a deceased individual, subject to the provisions of section 63 (2).

17.2. ***Mandatory protection of the commercial information of a third party***, if the record contains:

17.2.1. Trade secrets of that party;
17.2.2. Financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interest of that third party;
17.2.3. Information disclosed in confidence by a third party, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;
17.2.4. Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.

17.3. ***Mandatory protection of certain confidential information of third party***, where the head of a private body must refuse a request for access to a record of the body if its disclosure would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement.

17.4. ***Mandatory protection of the safety of individuals and the protection of property***, where such disclosure could endanger the life or physical safety of an individual, or prejudice or impair the security of:

17.4.1. a building, structure, or any system
17.4.2. a means of transport, or
17.4.3. any other property.

© MJSC (Pty) Ltd

17.5. ***Mandatory protection of records, which would be regarded as privileged from production in legal proceedings***.

17.6. ***Commercial information of private body***, in that a request for access to a record may be refused if the record contains:

17.6.1. trade secrets, financial, commercial, scientific, or technical information of the institution, which disclosure, could likely cause harm to the financial or commercial interest of the institution;
17.6.2. Information which, if disclosed could prejudice or put the institution at a disadvantage in negotiations or commercial competition; and
17.6.3. A computer program which is owned by the institution, and which is protected by copyright.

17.7. ***Mandatory protection of research information of the institution***. A request will be refused if this disclosure would disclose the identity of the institution, the researcher or the subject matter of the research and would place the researcher at a serious disadvantage.

17.8. ***Mandatory disclosure in public interest***. Despite any of the protections mentioned above, the Director of the Company shall grant a request for access to a record if:

17.8.1. the disclosure of the record would reveal evidence of-

17.8.1.1. a substantial contravention of, or failure to comply with, the law; or
17.8.1.2. imminent and serious public safety or environmental risk; and

17.8.2. the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.

18. APPEAL - REMEDIES

18.1. The Company does not have an internal appeal procedure. As such, the decision made by the Information Officer of the Company is final and requesters will have to exercise such external remedies at their disposal if the request for information is refused and the requester is not satisfied with the answer supplied by the Information Officer of the Company.
18.2. If a requester is aggrieved by the refusal of the Information Officer to grant a request for a record, the requester may, within thirty (30) days of notification of the Information Officer's decision, apply to court for appropriate relief.
18.3. The court will review the request and decide whether in fact the Information Officer of the Company should give the requester the information requested or not. A court hearing an application in terms of the PAIA Act may grant any order that is just and equitable including orders:

18.3.1. confirming, amending, or setting aside the decision which is the subject of the application;

© MJSC (Pty) Ltd

18.3.2. requiring the Deputy Information Officer of the Company or relevant authority of a public body or the head of a private body to take such action or to refrain from taking such action, as the court considers necessary within the period mentioned in the court order;

18.3.3. granting an interdict, interim or specific relief, a declaratory order or compensation; or

18.3.4. granting an order as to costs.

19. PROHIBITIONS OF SPECIAL PERSONAL INFORMATION

A responsible party may not process personal information concerning:

19.1. Religious or philosophical believes, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

19.2. The criminal behaviour of a data subject to the extend that such information relates to the alleged commission by the data subject of any offence and any proceedings in respect of the offense allegedly committed.

Unless such information forms part of public interest or record or deemed required by a Court of Law.

A data subject can provide written permission for the responsible person to declare or make public such information.

Information must be processed and supplied in all cases as mentioned hereto where such information forms part of a legislative requirement and / or in the interest of the party required, such as Trade Union information, registered institutions, etc.

20. DESTRUCTION OF INFORMATION

20.1. Information destruction must be reviewed at the level of requirements as set out by POPIA as well as the security safeguards of such information.

20.2. It is not sufficient to destroy or shred information internally that is deemed or classified under level 2 as per below. It is recorded that the Company will be deemed uncompliant where such structures are not correctly followed:

20.2.1. **Protection class 1**

- Normal security for internal data (such as paper with no confidential information, printing plates, etc.)
- **Security level: DIN P-1, DIN P-2, DIN P-3**
- Classification Level 1 being protected by Security Level 1 or 2 methods – in other words a traditional ribbon or strip cut shredding process is inadequate for POPI Act needs

20.2.2. **Protection class 2**

- High security for confidential data such as “Unauthorised disclosure would have serious effects” and “may lead to violations of laws or contractual

© MJSC (Pty) Ltd

obligations". At Classification Level 2 protection of personal data will meet "stringent requirements".

- **Security level: DIN P-3, DIN P-4, DIN P-5**

20.2.3. **Protection class 3**

- Very high protection for confidential and secret data addresses confidential and secret information where unauthorised disclosure would have "serious existence-threatening effects" and protection of personal data will be absolutely guaranteed.
- Security Levels 4 to 7 should be used for the highest Classification Level 3 information destruction
- **Security level: DIN P-4, DIN P-5, DIN P-6, DIN P-7**

20.3. The POPIA requires a business to use a Cross-Cut Shedder, (P-3 or P-4) or a Micro-Cut Shredder (P-5) and to be really safe, use a Super Micro-Cut Shredder (P-6) or a Super Fine Micro-Cut Shredder (P-6+).

21. FIC 8 DIRECTIVE

21.1. The purpose of this policy is to confirm the organisation's commitment to implementing an effective Anti-Money Laundering & Counter -Terrorist Financing Risk Management and Compliance Programme ("AML & CTF RMCP"), as required by FICA. The purpose of this AML & CTF Risk Management and Compliance Programme is to:

21.1.1. Enable the organisation to identify, assess, mitigate, manage and monitor the risk that the provision by the organisation of its products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities.

21.1.2. Provide for the manner in which the organisation determines if a person is a prospective client in the process of establishing a business relationship or entering into a single transaction with the organisation, or a client who has established a business relationship or entered into a single transaction, is a client of the organisation.

21.1.3. Provide for the manner in which the organisation complies with the compliance obligations of not establishing a business relationship or concluding a single transaction with an anonymous client or a client with an apparent false or fictitious name.

© MJSC (Pty) Ltd

21.1.4. Provide for the manner in which, and the processes by which, the organisation:

- Establishes and verifies the identity of a client, and FIC.
- Establishes a client representative's authority to establish a business relationship; or
- To conclude a single transaction on behalf of a client.

21.1.5. Provide for the manner in which, and the processes by which, the organisation determines whether future transactions that will be performed in the course of the business relationship, are consistent with the organisation's knowledge of a prospective client.

21.1.6. Provide for the manner in which, and the processes by which, the organisation conducts additional due diligence measures in respect of legal persons, trusts and partnerships.

21.1.7. Provide for the manner in which, and the processes by which, ongoing due diligence and account monitoring in respect of business relationships are conducted by the organisation.

21.1.8. Provide for the manner in which the examining of:

- Complex or unusually large transactions, and
- Unusual patterns of transactions which have no apparent business or lawful purpose takes place.

21.1.9. Provide for the manner in which, and the processes by which, the organisation will confirm information relating to a client when the organisation has doubts about the veracity of previously obtained information.

21.1.10. Provide for the manner in which, and the processes by which the organisation will perform the client due diligence requirements in accordance with the following compliance obligations:

- The identification of clients and other relevant persons,
- Understanding and obtaining information on business relationships,
- Additional due diligence measures relating to legal persons, trusts and partnerships,

© MJSC (Pty) Ltd

- Ongoing due diligence when, during the course of a business relationship, the organisation suspects or knows that a transaction or activity is suspicious or unusual.

21.1.11. Provide for the manner in which the organisation will terminate an existing business relationship where the organisation is unable to:

- Establish and verify the identity of a client or other relevant person,
- Obtain information describing the nature of the business relationship, the intended purpose of the business relationship concerned and the source of funds which a prospective client expects to use in concluding transactions in the course of the business relationship concerned.
- Conduct ongoing due diligence.

21.1.12. Provide for the manner in which, and the processes by which, the organisation will determine whether a prospective client is a foreign prominent public official or a domestic prominent influential person.

21.1.13. Provide for the manner in which, and the processes by which, enhanced due diligence is conducted for higher-risk business relationships and when simplified client due diligence might be permitted in the organisation.

21.1.14. Provide for the manner, place in which and the period for which client due diligence and transaction records are kept.

21.1.15. Enable the organisation to determine when a transaction or activity is reportable to the FIC.

21.1.16. Provide for the processes for reporting information to the FIC.

21.1.17. Provide for the manner in which:

- The AML & CTF RMCP is implemented in branches, subsidiaries or other operations of the organisation in foreign countries so as to enable the organisation to comply with its compliance obligations under FICA.
- The organisation will determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under FICA.

© MJSC (Pty) Ltd

- The organisation will inform the FIC and supervisory body concerned, if the host country does not permit the implementation of measures required under FICA.

21.1.18. Provide for the processes for the organisation to implement its AML & CTF RMCP.

21.1.19. Indicate if any of the processes are not applicable to the organisation, and if so, the reasons why it is not applicable.

22. STANDARDISED COMPLIANCE RISK AND IMPLEMENTED CONTROLS

The organisation has identified nine compliance risks considering its compliance objectives and obligations. The compliance risks have been assessed and evaluated based on the likelihood of the risk occurring, as well as the potential impact should the risk event occur.

Compliance Risk	Possible Noncompliance Sanctions	Likelihood Assess	Impact Assessment	Risk Rating	Implemented Controls
Civil or criminal fines or penalties where there is a failure in the FICA Reporting Duty procedures	Guilty of an Offence: Period not exceeding 15 years imprisonment or to a fine not exceeding R100 Million and / or Administrative Sanction: Financial Penalty not exceeding R10 Million in respect of natural persons and R50 Millions in respect of any other legal person	Possible	Catastrophic	Very High	▪ FICA Awareness Training ▪ Employee Reporting Procedure
Loss of sales and customer confidence where there is a failure in the FICA Reporting Duty procedures	Administrative Sanction: The restriction or suspension of certain specified business activities	Possible	Major	High	FICA Awareness Training Employee Reporting
Civil or criminal fines or penalties where proper FICA Customer Due Diligence measures are not conducted	Administrative Sanction: Financial Penalty not exceeding R10 Million in respect of natural persons and R50 Million in respect of any other legal person	Possible	Major	High	FICA Awareness Training Customer Due Diligence Forms

© MJSC (Pty) Ltd

Civil or criminal fines or penalties where FICA Recordkeeping requirements are not met	Administrative Sanction: Financial Penalty not exceeding R10 Million in respect of natural persons and R50 Millions in respect of any other legal person	Possible	Major	High	FICA Awareness Training
Reputational fallout or brand damage where there is a failure in the FICA Reporting Duty procedure	Administrative Sanction: A Reprimand	Possible	Moderate	Tolerable	FICA Awareness Training Employee Reporting
Civil or criminal fines or penalties where proper FICA GRC Standards are not implemented, reviewed and maintained	Administrative Sanction: Financial Penalty not exceeding R10 Million in respect of natural persons and R50 Millions in respect of any other legal person	Unlikely	Major	Tolerable	Annual Review of AML & CTF RMCP
Loss of sales and customer confidence where proper FICA GRC Standards are not implemented, reviewed and maintained	Administrative Sanction: The restriction or suspension of certain specified business activities	Unlikely	Major	Tolerable	Annual Review of AML & CTF RMCP
Reputational fallout or brand damage where proper FICA GRC Standards are not implemented, reviewed and maintained	Administrative Sanction: A Reprimand	Unlikely	Moderate	Low	▪ Annual Review of AML & CTF RMCP
Reputational fallout or brand damage where FICA Awareness Training of employees is not regularly conducted	Administrative Sanction: A Reprimand	Unlikely	Minor	Low	FICA Awareness Training

In order to do so and for every transaction, the company and any employee will need to obtain the following information:

© MJSC (Pty) Ltd

23. FRAUD PROCESS

After obtaining the above information and further upon conducting the following:

RISK RATING

This checklist must be completed with every FICA related Transaction.

Client name

Representative

Date

	Low	Medium	High
Product type			
Business Activity			
Client Attributes (are they on the UN list/ see Politically exposed check list			
Duration of client relationship (if single transaction is auto high)			
Jurisdiction of Client (if local then low/ if foreign then high)			
Transaction Value			
Type of Entity			
Source of fund			

Do note that should any of the above be deemed to be high risk then addition information regarding the source of the finds, the income to profile the client accordingly. This transaction must be authorised by the FICA compliance officer.

Additional Information

© MJSC (Pty) Ltd

23.1. After completing the risk rating and should the risk rating be high it will need to authorised by the FICA compliance officer, thereafter the following will need to be done;

23.1.1. The customer must provide a bank certificate or comparable institution containing the correct account information;
23.1.2. The employee conducting the sale must confirm the account information as well as details of the sale with the customer, this confirmation must be obtained before proceeding;
23.1.3. Only upon receipt of the information and confirmation thereto may the sale be confirmed by a superior at the company and thereafter actioned.

24. DISCIPLINARY ACTION

24.1. Where a FICA related complaint or an investigation related to an infringement of FICA or the organisation's AML & CTF RMCP has been finalised, the organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in noncompliance. In the case of ignorance or minor negligence, the organisation will undertake to provide further FICA Awareness training to the employee.

24.2. Any gross negligence or the wilful noncompliance, will be considered a serious form of misconduct for which the organisation 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:

24.3. A recommendation to commence with disciplinary action.

24.3.1. A referral to appropriate law enforcement agencies for criminal investigation.
24.3.2. Recovery of funds and assets in order to limit any prejudice or damages caused.

Duly so undersigned and implemented at Table View on this 12th day of March 2024

_____

M. Mendonca

OWNER / DIRECTOR

© MJSC (Pty) Ltd

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

TO: The Information Officer

_____

_____

_____

_____ *(Address)*

E-mail address: _____

Fax number: _____

*Mark with an **"X"***

☐ Request is made in my own name ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full Names				
Identity Number				
Capacity in which request is made *(when made on behalf of another person)*				
Postal Address				
Street Address				
E-mail Address				
Contact Numbers	Tel. (B):		Facsimile:	
	Cellular:			
Full names of person on whose behalf request are made *(if applicable):*				
Identity Number				
Postal Address				

© MJSC (Pty) Ltd

Street Address				
E-mail Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			

PARTICULARS OF RECORD REQUESTED

Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)

Description of record or relevant part of the record:	
Reference number, if available	
Any further particulars of record	

TYPE OF RECORD
*(Mark the applicable box with an "**X**")*

Record is in written or printed form	

© MJSC (Pty) Ltd

Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	
FORM OF ACCESS *(Mark the applicable box with an "**X**")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

MANNER OF ACCESS *(Mark the applicable box with an "**X**")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

© MJSC (Pty) Ltd

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	
Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a) *A request fee must be paid before the request will be considered.* *b)* *You will be notified of the amount of the access fee to be paid.* *c)* *The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.* *d)* *If you qualify for exemption of the payment of any fee, please state the reason for exemption*	
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	**Facsimile**	**Electronic communication *(Please specify)***

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Requester / person on whose behalf request is made

---

FOR OFFICIAL USE

© MJSC (Pty) Ltd

Reference number:	
Request received by: *(State Rank, Name And Surname of Information Officer)*	
Date received:	
Access fees:	
Deposit (if any):	

_____

Signature of Information Officer

© MJSC (Pty) Ltd

FORM 3
OUTCOME OF REQUEST AND OF FEES PAYABLE

[Regulation 8] *Note:*

1. *If your request is granted the—*
   (a) amount of the deposit, (if any), is payable before your request is processed; and
   (b) requested record/portion of the record will only be released once proof of full payment is received.
2. *Please use the reference number hereunder in all future correspondence.*

Reference number: _____

TO: _____

_____

_____

_____

Your request dated _____, refers.

1. You requested:

Personal inspection of information at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)* is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees prescribed in Annexure B.	

OR

2. You requested:

Printed copies of the information *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of information on flash drive *(including virtual images and soundtracks)*	
Copy of information on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

3. To be submitted:

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language: *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

© MJSC (Pty) Ltd

Kindly note that your request has been:

☐ Approved

☐ Denied, for the following reasons:

4. Fees payable with regards to your request:

Item	Cost per A4-size page or part thereof/item	Number of pages/items	Total
Photocopy			
Printed copy			
For a copy in a computer-readable form on: (i) Flash drive • To be provided by requestor (ii) Compact disc • If provided by requestor • If provided to the requestor	R40.00 R40.00 R60.00		
For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on the quotation of the service provider		
Copy of visual images			
Transcription of an audio record, per A4-size	R24.00		
Copy of an audio record (i) Flash drive • To be provided by requestor (ii) Compact disc • If provided by requestor • If provided to the requestor	R40.00 R40.00 R60. 00		
Postage, e-mail or any other electronic transfer:	Actual costs		
TOTAL:			

5. Deposit payable (if search exceeds six hours):

☐ Yes ☐ No

Hours of search		Amount of deposit *(calculated on one third of total amount per request)*	

© MJSC (Pty) Ltd

The amount must be paid into the following Bank account:

Name of Bank: _____
Name of account holder: _____
Type of account: _____
Account number: _____
Branch Code: _____
Reference Nr: _____
Submit proof of payment to: _____

Signed at _____ this _____ day of _____ 20 _____

_____
Information officer

© MJSC (Pty) Ltd

INTERNAL APPEAL FORM

FORM 4

[Regulation 9]

Reference Number: **…….**

PARTICULARS OF PUBLIC BODY				
Name of Public Body				
Name and Surname of Information Officer:				
PARTICULARS OF COMPLAINANT WHO LODGES THE INTERNAL APPEAL				
Full Names				
Identity Number				
Postal Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
E-Mail Address				
Is the internal appeal lodged on behalf of another person?	Yes		No	
If answer is "yes", capacity in which an internal appeal on behalf of another person is lodged: *(Proof of the capacity in which appeal is lodged, if applicable, must be attached.)*				
PARTICULARS OF PERSON ON WHOSE BEHALF THE INTERNAL APPEAL IS LODGED ***(If lodged by a third party)***				
Full Names				
Identity Number				
Postal Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
E-Mail Address				

© MJSC (Pty) Ltd

DECISION AGAINST WHICH THE INTERNAL APPEAL IS LODGED *(mark the appropriate box with an "X")*	
Refusal of request for access	
Decision regarding fees prescribed in terms of section 22 of the Act	
Decision regarding the extension of the period within which the request must be dealt with in terms of section 26(1) of the Act	
Decision in terms of section 29(3) of the Act to refuse access in the form requested by the requester	
Decision to grant request for access	

GROUNDS FOR APPEAL *(If the provided space is inadequate, please continue on a separate page and attach it to this form. all the additional pages must be signed)*	
State the grounds on which the internal appeal is based:	
State any other information that may be relevant in considering the appeal:	

You will be notified in writing of the decision on your internal appeal. Please indicate your preferred manner of notification:

Postal address	Facsimile	Electronic communication *(Please specify)*

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Appellant/Third party

© MJSC (Pty) Ltd

FOR OFFICIAL USE

OFFICIAL RECORD OF INTERNAL APPEAL

Appeal received by: *(state rank, name and surname of Information Officer)*				
Date received:				
Appeal accompanied by the reasons for the information officer's decision and, where applicable, the particulars of any third party to whom or which the record relates, submitted by the information officer:		Yes		
		No		
OUTCOME OF APPEAL				
Refusal of request for access. Confirmed?	Yes		New decision *(if not confirmed)*	
	No			
Fees (Sec 22). Confirmed?	Yes		New decision *(if not confirmed)*	
	No			
Extension (Sec 26(1)). Confirmed?	Yes		New decision *(if not confirmed)*	
	No			
Access (Sec 29(3)). Confirmed?	Yes		New decision *(if not confirmed)*	
	No			
Request for access granted. Confirmed?	Yes		New decision *(if not confirmed)*	
	No			

Signed at _____ this _____ day of _____ 20 _____

_____

Relevant Authority

© MJSC (Pty) Ltd