z

MAPTTE (PTY) LTD

LEGISLATIVE & COMPLIANCE FRAMEWORKS WITH INTERNAL POLICIES FOR THE PROTECTION OF PERSONAL INFORMATION

This framework outlines the processes and related policies and procedures in the pursuit of compliance within the Protection of Personal Information Act of 2013 (POPIA).

This POPIA Framework must be read with the legislative framework already provided as background and it must be seen as one document.

The purpose of this framework is to enable the FSP to:
To ensure compliance with all applicable legislation regarding the protection of personal information of identifiable individuals (employees, clients and other third parties).
Follow the principles of good practice and treating clients fairly.
Protect the FSP and the individuals on whose behalf data is collected, processed, distributed, disclosed, and stored.
Protect the FSP from the consequences of a breach and related fines and penalties.
Personal Information: This framework applies to the protection of personal information (note definition of personal information in legislative framework) relating to identifiable individuals, both natural and juristic.
Framework (Policy) Statement: The FSP will:
Endeavor to comply with the legal requirements of POPIA and the relevant Regulations as well as the principles of good practise and treating clients fairly.
Respect individuals' rights to privacy and the protection of their personal information (data) which is collected, processed, distributed, disclosed, and held by the FSP.
Be open and honest with the relevant individuals whose personal information (data) is collected, processed, distributed, disclosed, and held.
Provide training and support to all employees who deals with personal information so that they can act confidently and consistently.

The FSP recognises that it is the first priority of POPIA to avoid causing harm to individuals. Therefor it will endeavour to:
Keep information (data) securely in the right hands; and
Retain good quality information (data).

The scope of framework applies to all the operations and business practices of the FSP wherever it is conducted but based at the registered offices and branches. It applies to all employees as per the effective date.

As the Key Individual of the mentioned, FSP, I Thenjiswa Mbewu, hereby confirm the adoption of these frameworks and policies as part of the FSP's internal control structure and procedures.

_____
Key Individual Signature
Thenjiswa Mbewu

Date: 30 Nov 2023

No TABLE OF CONTENTS

1. DOCUMENT DETAILS

1.1 Background:

This POPIA Manual provides a compliance framework and internal policies and procedures for meeting the legislative requirements in terms of the protection of personal information and to manage the associated compliance risks effectively and efficiently. The framework will ensure the appropriateness and consistency of approach between the external compliance requirements and internal policies and procedures. It is used to establish a structured approach to continuously improve the many technical and complex requirements of the Protection of Personal Information Act.

1.2 Purpose & Objective:

A POPIA compliance framework provides a monitoring capability to manage compliance with the obligations of the Protection of Personal Information Act to ensure compliance with the conditions for the lawful processing of personal information.

The Information Regulator has extended the duties and responsibilities to ensure a suitable compliance framework is implemented. Responsible parties will have to demonstrate compliance to a wide range of legal obligations that include:

- keeping documentation that can be used later to demonstrate accountability
- clarifying the roles, responsibilities and accountability obligations of responsible parties using risk-based approaches to data protection and the implementation of protective measures which correspond to the level of risk of processing personal data so that the fundamental rights and freedoms of data subjects are protected
- supporting information officers and their efforts to achieve strong data protection compliance and establish effective privacy programmes
- providing effective governance of processors and third parties operating under the authority of the responsible party
- pro-actively identifying and tracking procedural or training weaknesses in an effort to preclude regulatory violations.

1.3 Document Approval:

Effective Date	Version	Authorised Person	Role	Management Approved
01/04/2020	V1	Thenjiswa Mbewu	KI	

1.4 Revision History:

Effective Date	Version	Description of Change	Management Approved
30/11/2023	V2	Amendments	Thenjiswa Mbewu

The date listed in the first line of the Revision History table; is the date the document received its final approval. Hereafter, the date becomes the revision date, displayed as the Effective Date.

2. LEGISLATIVE FRAMEWORK:

2.1 What is POPIA:

The intention of the Protection of Personal Information Act (POPIA) is to bring South Africa in line with international standards of protection of personal information and will radically change the way in which both government and business deal with individuals' private information. POPIA sets conditions for what companies and individuals must and may do with personal information about their employees, clients and other third parties.

2.2 Personal Information:

The definition of personal information is all encompassing and includes biometric information. Basically, if information can identify someone, it is deemed personal. In the financial services industry, Financial Service Providers and their staff receive (as an example) application forms, claims and premiums data that contain a host of information such as names, identity numbers, staff numbers, addresses, tax numbers, banking details, health information etc. All of this is personal information, so POPIA is applicable to all FSP's.

2.3 Important Definitions:

• 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.
• Consent: means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.
• Data Subject: means the person to whom personal information relates.
• De-identify: means to delete all information that identifies the data subject.
• Information Officer: in relation to a private body means the head of a private body or any person duly authorised by that person.
• Operator: means 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.
• Personal Information: means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.
• Person: a natural or juristic person.
• Processing: means any operation or activity or any set of operations, whether or not by automatic means, concerning personal Information
• Public Record: means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
• Regulator: means the Information Regulator.
• Re-identify: means to resurrect any information that has been de-identified, that identifies the data subject.
• Record: means any recorded information regardless of form or medium.
• Responsible Party: means 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.
• Special Personal Information: the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. The prohibition on processing special personal information does not apply if the processing is carried out with the consent of a data subject or if processing is necessary for the establishment, exercise or defence of a right or obligation in law or information has deliberately been made public by the data subject.

2.4 Rights of Data Subjects:

A Data Subject has the right to -

• have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information including the right to be notified that—
- personal information about him, her or it is being collected; and
- his, her or its personal information has been accessed or acquired by an unauthorised person.

• establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information.
• request, where necessary, the correction, destruction or deletion of his, her or its personal information.
• object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information.
• object to the processing of his, her or its personal information at any time for purposes of direct marketing.

2.5Conditions for Data Collection:

Condition 1: Accountability:

The FSP must ensure that all principles and measures of the Act are complied with during the collection and processing of personal information.

Condition 2: Processing limitation:

Processing must be done lawfully and not infringe the privacy of the individual. Processing of personal information must be adequate, relevant and not excessive, given the purpose for which it is to be used. Personal information may only be processed –
• if the data subject or a competent person where the data subject is a child consent to the processing.
• processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party.
The responsible party bears the burden of proof for the data subject's or competent person's consent. The data subject or competent person may withdraw his, her or its consent at any time or object to the processing of personal information and the responsible party may then no longer process the personal Information. Personal information must be collected directly from the data subject unless –
• the information is contained in or derived from a public record or has deliberately been made public by the data subject.
• the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source.

Condition 3: Purpose Specification:
Personal information must only be collected for a specific purpose and the individuals must be aware of this. Records must not be kept for longer than necessary to achieve the purpose for which it was collected. Legislative requirements (FICA & FAIS) must be adhered to. A responsible party must destroy or delete a record of personal information as soon as reasonably practicable after the responsible party is no longer authorised to retain the record. It must be done in a manner that prevents its reconstruction in an intelligible form.

Condition 4: Further Processing Limitation:

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in the first place. The responsible party must take account of —
• the relationship between the purpose of the intended further processing and the purpose for which the information has been collected.
• the nature of the information concerned.
• the consequences of the intended further processing for the data subject.

• the manner in which the information has been collected.
• any contractual rights and obligations between the parties.

Condition 5: Information Quality:

The holder of the data must take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary, always taking into account the purpose for which the information was initially collected or further processed.

Condition 6: Openness:

A responsible party must maintain the documentation of all processing operations under its responsibility. The responsible party must take reasonably practicable steps to ensure that the data subject is aware of —
• the information being collected or the source from which it is collected.
• the name and address of the responsible party.
• the purpose for which the information is being collected.
• whether or not the supply of the information is voluntary or mandatory.
• the consequences of failure to provide the information.
• any particular law authorising or requiring the collection of the information.
• the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.

Conditions 7: Security Safeguards:

A responsible party must secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent —
• loss of, damage to or unauthorised destruction of personal information.
• unlawful access to or processing of personal information. An operator or anyone processing personal information on behalf of a responsible party or an operator, must process such information only with the knowledge or authorisation of the responsible party.
Condition 8: Data Subject Participation:
The data subject can request whether an organisation holds their private or personal information, and what information is held. They may also request a responsible party to correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. The responsible party must adhere to the request of the data subject as soon as possible and inform the data subject of the action taken as a result of the request.

2.6Special Personal Information:

The following information may not be processed without consent of the data subject or unless allowed by law – (a) Religious or philosophical beliefs (b) Race or ethnic origin (c) Trade union membership (d) Political persuasion (e) Health or sex life (f) Biometric information (g) Criminal behaviour relating to alleged offences.

2.7Children:
No personal information of a child (under 18) may be processed without consent of a competent person or unless allowed by law.

2.8Information Regulator and Information Officer:

The information regulator's powers, duties and functions in terms of POPIA are –
(a) to educate
(b) to monitor and enforce compliance
(c) to consult
(d) to handle complaints
(e) to conduct research and report to parliament
(f) to issue codes of conduct
(g) to facilitate cross-border co-operation
(h) other general duties for example matters relating to the access of information as provided by PAIA.

In light of the duties imposed by POPIA it is recommended that FSP's decide on the appointment of an information officer (and deputy information officer where appropriate). Registration of Information Officers with the Regulator is a prerequisite for Information Officer to take up their duties in terms of POPIA and PAIA.

An information officer's responsibilities include —
- the encouragement of compliance with the conditions for the lawful processing of personal information.
- dealing with requests made pursuant to this Act.
- working with the Regulator in relation to investigations.
- ensuring compliance with the provisions of this Act.

The duties of information officers out that an information officer must –
• develop, implement and monitor a compliance framework.
• ensure that adequate measures and standards exist.
• conduct preliminary assessments.
• develop a manual for the purpose of the Promotion of Access to information Act and the POPl Act.
• develop internal measures and adequate systems to process requests for access to information.
• conduct awareness sessions.

Information officers must take up their duties after the responsible party has registered them with the Regulator. The POPIA information officer would be –

• In the case of a sole practitioner - the sole practitioner or any person duly authorised by the sole practitioner.
• in the case of a partnership - any partner of the partnership or any person duly authorised by the partnership.
• In the case of an incorporated practice - the chief executive officer or a person duly authorised by the chief executive officer.

One of the primary functions of the information officer is the receipt, processing and determining whether access to information held by the private body should be granted.

A Deputy Information Officer(s) should have a reasonable understanding of the business operations and processes of a body.

2.9Prior Authorization:

Prior authorisation is necessary where the responsible party plans to process information –

• which contains any unique identifiers of data subjects for a purpose other than the one specifically intended at collection and with the aim of linking the information being processed with information processed by other responsible parties.
• in respect of criminal, unlawful or objectionable conduct.
• for the purpose of credit reporting.
• that is defined as special personal information or is the information of a child which is being transferred to a foreign country that does not provide an adequate level of protection in its law.

The Regulator may require prior authorisation if the processing carries a risk to the legitimate interests of the data subject. The authorisation only has to be obtained once for a particular category of processing but if the manner of processing changes then a further application to the Regulator for authorisation will be necessary.

2.10 Consequences of Infringement:

POPIA makes provision for enforcement notices to be served on those infringing the data protection principles or the direct marketing provisions of POPI. Failure to comply with an enforcement notice is an offence, and on conviction may lead to a fine of not more than R10 million, or up to 10 years in prison, or both.

2.11 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 make a donation of any kind for any reason.

2.12 Section 72 of POPIA requires that in order for cross-border transfers of personal information to be permissible, one of the following must be present:

Adequate legal protection: The recipient of the personal information must be subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that effectively upholds the principles for reasonable processing, and that include provisions that are substantially similar to the conditions for the lawful processing of personal information and for the further transfer of personal information.
Consent: The data subject consents to the transfer.
Necessary for the performance of a contract: The transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request.
Interests of the data subject: The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.
Benefit of the data subject: The transfer is for the benefit of the data subject in circumstances where it is not reasonably practicable to obtain the consent of the data subject for the transfer, and the data subject would be likely to give consent had it been obtained.
These are not cumulative requirements, and only one of the above would need to be present in order for the cross-border data transfer to pass muster.

2.12 Staff Training and Acceptance of Responsibilities

Employees will be required to attend training, disciplinary actions will be taken against employees who do not comply with the provisions of the Act.

3.1 Key Risks:

The FSP has identified the following potential key risks, which this framework is designed to address:
External Breach of privacy and confidentiality with subsequent loss to the individual and the FSP via for example hacking etc.
Internal Breach of privacy and confidentiality with subsequent loss to the individual and the FSP via for example unauthorised access or unauthorised disclosure etc.
Consent process followed with individuals not meeting all requirements in terms of collecting, processing, distribution, disclosure, and storage of personal information with subsequent complaints received.
Other non-compliance issues leading to Regulatory action with subsequent fines and penalties.
Legal and compliance documentation such as employment contracts, service level agreements, application forms etc not brought in line with POPIA with subsequent accountability and responsibility issues.

The FSP will endeavour to comply with all relevant conditions of POPIA and related Regulations. To oversee the FSP's compliance in this regard an Information Officer is appointed and registered with the Information Regulator. Responsibilities of the Information Officer (which may be delegated to a Deputy Information Officer)

3.2 Impact Assessment

The FSP may apply an impact assessment on the business focussing on the following areas

ACCOUNTABILITY. Roles and responsibilities must be clearly set out both internally and when information is shared with third parties. Senior management must oversee IG and should delegate IG responsibilities to appropriate individuals (information custodians). Standards and procedures must be put in place to ensure that the level of IG can be audited.

STANDARDISATION. Business processes and activities must be well-defined and documented in an open and verifiable way. The documentation must be available to employees and appropriate third parties.

INTEGRITY. The right processes are in place to guarantee that the institutional information we use or manage is comprehensible, clear, consistent, and reliable

SECURITY. Confidential and personal information must be protected from unauthorised destruction, modification, or access.

COMPLIANCE. Good information governance promotes and facilitates compliance with internal policies, applicable legislation, or other binding rules.

AVAILABILITY. Information must be available to the appropriate people at the appropriate time.

RECORDS MANAGEMENT. Information will be retained for an appropriate time only, taking into account legal, regulatory, fiscal, operational, and historical requirements. Once the retention periods have passed, information is disposed of securely.

EMPOWERMENT**.** The Business' employees must be empowered through training to work responsibly with information and to protect it. In the process, they will empower their staff to protect their own privacy.

A. THE PROTECTION OF PERSONAL INFORMATION (POPI) ACT POLICY

The Protection of Personal Information (POPI) Act requires us to inform clients how we use and disclose Their personal information obtained from them. We are committed to protecting our clients privacy and will ensure that the clients personal information is used appropriately, transparently and according to applicable law. Your right to privacy and security is very important to us. We, Maptte treat personal information obtained as private and confidential and are committed to providing you with secure access to our services.

This Privacy Policy tells you how we will process and protect your personal information. It should be read together with our Terms of Service, which outlines what services we provide, how we provide our services and what we do with your personal information. It is important that you read, understand and accept our Terms of Service if you would like to use our services.

1.Personal information, in terms of the Protection of Personal Information Act, 4 of 2013 ("POPIA"), means "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person". South Africa's Constitution, Act 108 of 1996, provides that everyone has the right to privacy. This includes the right to protection against the unlawful collection, retention, dissemination and use of your personal information. Because of the sensitivity of some personal information, we ensure that the way we process your personal information complies fully with POPIA.

This Privacy Policy applies to any of your personal information that we collect and process through our websites, www.maptte.co.za and or which you authorise us to collect from third parties.

You will see that some of the words listed in this Privacy Policy are in italics. Those words are defined in POPIA and those definitions apply to this Privacy Policy. For example, under POPIA, you are defined as a data subject.

Our Privacy Policy terms may change from time to time. When we change them, the changes will be made on our website. Please ensure that you visit our website and regularly read this Privacy Policy. Although we do not promise to do so, we may give you notice of any changes we think are important.

2. Your rights under this Privacy Policy

You have the right to have your personal information processed lawfully. Your rights include the right:

- to be notified that your personal information is being collected or that your personal information has been accessed or acquired by an unauthorised person e.g. where a hacker may have compromised our computer system;
- to find out whether we hold your personal information and to request access to your personal information;
- to request us, where necessary, to correct, destroy or delete your personal information;
- to object, on reasonable grounds, to the processing of your personal information;
- to object to the processing of your personal information for purposes of direct marketing, including by way of unsolicited communications;
- not to be subject, in certain circumstances, to a decision which is based solely on the automated processing of your personal information;
- to submit a complaint to the Regulator if you believe that there has been interference with the protection of your personal information, or if you believe that an independent adjudicator who may be resolving your complaint against us, has not decided the matter correctly; and
- to institute civil proceedings against us if you believe that we have interfered with the protection of your personal information.

3.Types of personal information collected and how we collect it.

We collect and process clients personal information mainly to provide our clients with access to the services and products of the providers with whom we have contractual agreements in place and to help us improve our services to our clients. The type of information we collect may depend on the need for which it is collected and will be processed for that specific purpose only. Where possible, we will inform the client what information is required to be provided to us and what information is optional.

We collect and process your personal information mainly to provide you with access to our services and products (and all other activities and processes incidental thereto), to help us improve our offerings to you and for certain other purposes explained below.

The type of information we collect will depend on the purpose for which it is collected and used (processed). We will only collect information that we need for that specific purpose.

Examples of the personal information that we collect are as follows (but it is not limited to the examples provided):

Some of your information that we hold may include, your first and last name, identity number, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, marital status, details of a driving license, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance (including previous insurance and claims experience), income, expenditure, family history, medical information, telephone recordings of conversations, emails, your banking details, premiums paid and information relating to claims and other investigations (including reports and photos).

We collect information **directly from you**, where you provide us with your personal details, for example when you purchase a product or services from us or when you submit enquiries to us or contact us. Where possible, we will inform you what information you are required to provide to us and what information is optional.

We also collect information about you from other sources as explained below.

With your consent, we may also supplement the information that you provide to us with information we receive from other companies such as Product Providers or other Financial Services Providers, in order to offer you a more consistent and personalized experience in your interactions with us.

We will not intentionally collect and process the personal information of a child unless we have the permission of a competent person. The examples of Collection are summarized below (but it is not limited to the examples provided) -

- Our computer systems,
- Our website,
- Insurance, Investment, Customer Due Diligence and other Proposal and Application Forms,
- Previous and current Insurance, Investment or other Policies or Schedules (provided via Astute with your consent or by you directly),
- Claim Forms
- Telephone Calls,
- Emails,
- Credit Reference Agency via the relevant Product Provider/s,
- Business Partners such as Product Providers, Assessors, Brokers etc.
- Social Media Platforms such as What's Up, Face Book etc.

4. How we use your information

Given our aim to provide you with ongoing financial services, we would like to use your information to keep you informed about other financial products and services which may be of particular interest to you.

You may also give and withdraw consent and tell us what your communication preferences are.

We do not and will not sell personal information to a third party. We may disclose your personal information to our service or product providers who are involved in the delivery of products or services to you. We have agreements in place to ensure that they comply with these privacy terms.

We may share your personal information with, and obtain information about you from (read with examples of collection):

- Third parties for the purposes listed above, for example contracted product providers or insurers, astute, credit reference and fraud prevention agencies, law enforcement agencies, banks etc.,
- Other insurers to prevent fraudulent claims,
- Other companies (as mentioned above) when we believe it will enhance the services and products, we can offer to you, but only where you have not objected to such sharing,
- Other third parties from whom you have chosen to receive marketing information.
- Third parties or services providers such as IT providers, system administrators, collection agencies etc. that enables us to operate as a Close Corporation, a Financial Services Provider and an Accountable or Non-Accountable Institution.

5.How consent is obtained

In order to use our services, you need to accurately complete an number of internal forms and documents available from us. These forms requires that you to provide us with certain personal information which includes, but is not limited to, your names, email address, your identity number, proof of address, contact numbers, and proof of banking.
We also obtain your consent when you complete the forms allowing is to proceed with the business transaction.

If you do not agree to any part of this Privacy Policy, please complete form 1 and email to our information officer.

Please refer to our PAIA manual for the procedure to be followed if you wish to gain access to your personal information that we hold.

6. How we use your personal information

6.1. The personal information that we collect from you will be used to provide the following services:

We will use your personal information only for the purposes for which it was collected or agreed with you, note examples below (but it is not limited to the examples provided):

- To provide our products or services to you, to carry out the transaction you requested and to maintain our relationship,
- For underwriting purposes,
- To assess and process claims and to take recovery action,
- For collection of premiums via Collection Agencies
- To conduct credit reference searches or verification (including credit scoring, assessment and management)
- To confirm and verify your identity for security purposes and update your details,
- To perform customer due diligence or enhanced customer due diligence processes as required by the money laundering and terrorist financing legislative framework.
- For operational purposes, and where applicable, credit scoring and assessment and credit management,
- For purposes of claim checks,
- For the detection and prevention of fraud, crime, money laundering or other malpractice,
- For debt tracing or debt recovery,
- To conduct market or customer satisfaction research or for statistical analysis,

- Resolving complaints,
- For audit and record keeping purposes, and
- In connection with legal proceedings.

We will also use your personal information to comply with legal and regulatory requirements or industry codes to which we subscribe, or which apply to us, or when it is otherwise allowed by law.

We will only transfer your personal information outside the borders of South Africa with your consent and where the privacy legislation is of a high standard. We do not use your personal information for marketing purposes without your consent.

7.Retention, amendment and destruction of personal information

7.1. We only retain your personal information for a period necessary to achieve the purpose we collected it for, unless the longer retention of your personal information is required or authorised by law. Once we have achieved that purpose we will, as soon as reasonably practicable, destroy or delete the record of your personal information in accordance with the provisions of POPIA.

We are legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access and use of personal information. We will, on an ongoing basis, continue to review our security and risk management controls and related processes to ensure that your personal information is secure.

Our risk management (security) policies and procedures cover:

- Physical security,
- Computer and network security,
- Access to personal information,
- Secure communications,
- Security in contracting out activities or functions,
- Retention and disposal of information,
- Acceptable usage of personal information,
- Governance and regulatory issues,
- Monitoring access and usage of private information,
- Investigating and reacting to security incidents.

When we contract with third parties, we impose appropriate security, privacy and confidentiality obligations on them (our confidentiality agreements) to ensure that personal information that we remain responsible for, is kept secure.

We will ensure that anyone to whom we pass your personal information agrees to treat your information with the same level of protection as we are obliged to.

Personal Information is securely stored on administrative systems, computer systems, servers (in and outside South Africa), laptops, filing cabinets and one drive (cloud).

Your personal information is stored for a minimum of five years after the cancellation or termination of the transaction or business relationship in accordance with applicable legislation. We will take reasonable steps to destroy or de-identify your personal information when the law no longer requires us to retain or keep it.

7.2. It's important that your personal information is up to date and accurate.

8.Transfer of personal information to third parties

8.1. In order for us to carry out our obligations in terms of the services concluded between ourselves and you, we may need to pass your personal information on to third parties, such as our product providers. This Privacy Policy records your consent to us passing your personal information onto those third parties.

8.2. We will ensure that your personal information is processed in a lawful manner and that the third parties or we do not infringe your privacy rights. In the event that we ever outsource the processing of your personal information to a third party operator, we will ensure that the operator processes and protects your personal information using reasonable technical and organisational measures that are equal to or better than ours.

9.Where we store your personal information

9.1. Protecting your personal Information is very important to us. We store your information on a Structured Query Language ("SQL") Database within a Microsoft Server either hosted in the cloud in South Africa, or in KF's access controlled server room, behind a firewall.

10.Transborder transfer of personal information

10.1. We will not transfer any personal information collected from you outside the borders of South Africa.

10.2. In the event that we transfer or store your personal information outside South Africa, we will take all steps reasonably necessary to ensure that the third party who receives your personal information is subject to a law, binding corporate rulesor binding agreement which provides an adequate level of protection.

11.How we use cookies or other personal identification software

11.1. Our websites use cookies. Cookies are small software programmes that install themselves on your computer or your mobile device. They are intended to make your experience of visiting and navigating through our website easier and more pleasant. Cookies may collect personal information such as the identity of your computer or mobile device and your location.

11.2. If you do not want cookies to be installed on your computer or mobile device, please do not use our website. This means that you will not be able to use our services. By using our website, you consent to cookies, including Google Analytics, being installed on your computer or mobile device.

12. Information Security

12.1. We promise that we will secure the integrity and confidentiality of your personal information in our possession or under our control. We will do this by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of your personal information; and unlawful access to or processing of your personal information.
12.2. We have installed a firewall network security system to protect all your personal information that is stored in the cloud and on our premises. We have put in place managed security services which maintain and manage our firewall.

12.3. We have also restricted the number of persons who can access your personal information to only our staff members that are required to work on your personal information.

12.4. While we will take every reasonable measure to protect your personal information, it is very important that you maintain control over your account and or information. You should prevent anyone from accessing your account or information by not disclosing your account details i.e. usernames, passwords or any information associated with your account.

Objecting to the processing of data for advertising purposes

Users have the right to object at any time to the processing of personal data for direct marketing purposes. If a User objects, Maptte Insurance Brokers will no longer process such personal data. Objections must be addressed to our Deputy Information Officer. Her details are provided below.

Business contact via our website

If a User is a business contact that has provided MaptteMaptteMaptte with personal data, we will store such personal data in our database so that it is able to follow up on previous business conversations held with the User, provide additional information to the User concerning our services and/or assist the User in related services.

Email / direct mail campaign data

From time to time, Maptte Insurance Brokers may contact its clients (Users) directly by mail, email, or telephone to provide information concerning new products and services. We will, however, not contact a User with any commercial communications that are unrelated to the services provided by LVM Insurance Brokers. When responding to one of these campaigns, Users may elect to provide us with personal information which will be used for the purpose indicated.

Survey data

From time to time, we may conduct surveys in respect of our service delivery. Participation in these surveys is optional. If, however, Users respond to one of the surveys, Users may elect to provide LVM Insurance Brokers with personal information. Unless a User otherwise consents, we will only use the information to determine the type/s of services that may be of interest to the User and to operate and improve its service offerings.

Policy amendments

We may amend and/or update these standard terms and conditions at any time. Users are encouraged to frequently check our website for the purposes of familiarizing themselves with these standard terms and conditions, particularly in so far as they relate to the protection of personal information. Users acknowledge and agree that it is their responsibility to review these standard terms and conditions periodically and become aware of any amendments and/or updates.

Sale of business

In the event of a change in control of Maptte is acquired by another company), or preliminary discussions to that end, the personal data of Users may be included in order that the acquirer may continue to effectively serve both Users and clients.

Acceptance of standard terms and conditions

By using Maptte website, the User signifies acceptance of these standard terms and conditions. If a User does not agree to these terms and conditions, he/she is advised not to use our website. The continued use of the website by Users following the posting of updates and/or amendments to these standard terms and conditions will be deemed to be an acceptance by such User of such updates and/or amendments.

Contacting Maptte

If a User has any questions concerning these standard terms and conditions and/or the practices and/or dealings of Maptte website, kindly contact our Deputy Information Officer. Her details are provided below.

13. The law governing this privacy policy

This privacy policy is governed by the laws of the Republic of South Africa. Any dispute arising out of this privacy policy will be resolved in a South African court.

Every person whose personal information we process has the following rights:

- You have the right to request copies of your personal information, subject to the terms and conditions described in our Promotion of Access to Information ("PAIA") manual and our POPIA Policy which is available on request.
- You have the right to request that we correct any information you believe is inaccurate,
- You have the right to request that we erase your personal information, under certain conditions,
- You have the right to object to us processing your personal information, under certain conditions
- You have the right to lodge a complaint with the Information Regulator whose contact details is in our PAIA Manual and POPIA Policy.

If you wish to object to the processing of personal information or if you wish to request for correction or deletion of personal information, then please complete Form 1 or Form 2 at the end of this privacy notice.

14. How to contact us

14.1. If you have questions and/or comments about our privacy policy or need to protect any of your rights set out in this policy, please contact our information officer on email address info@maptte.co.za or telephone number 010 015 5765

14.2. Our physical address is The Office Zone@Foresthill, 24 Marie Rd, Centurion, 0157.

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION N 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, 2018
[Regulation 2]

Note:

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

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique Identifier / Identity Number	
Residential, postal or business address: Contact number(s):	
	Code ( )
Contact number(s)	
Fax number / E-Mail address:	
B	**DETAILS OF RESPONSBILE PARTY**
Name(s) and surname / Registered name of responsible party:	
Residential, postal or business address:	
Residential, postal or business address: Contact Number(s)	
	Code ( )
Fax number / E-Mail address:	
C	**REASONS FOR OBJECTION INTERMS OF SECTION 11 (1)(d) to (f) (Please provide detailed reasons for the objection)**

Signed at …… this ……. Day of …….. 20……..

……
Signature of data subject / designated person

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION 2018
[Regulation 3]

Note:

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

Mark the appropriate box with an "X".

Request for:

□ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

□ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique Identifier / Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-Mail address:	
B	**DETAILS OF RESPONSBILE PARTY**
Name(s) and surname / Registered name of responsible party:	

Residential, postal or business address:	
	Code ( )
Contact Number(s)	
Fax number / E-Mail address:	

C	INFORMATION TO BE CORRECTED/DELETED/DESTRUCTED/ DESTROYED
D	**REASONS FOR "CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSBILE PARTY IS NO LONGER AUTHORISED TO RETAIN.** **(Please provide detailed reasons for the request)**

Signed at …… this ……. Day of …….. 20……..

…….
Signature of data subject / designated person

B. THE PROTECTION OF PERSONAL INFORMATION (POPI) ACT DISCLOSURE AND CONSENT TO OBTAIN INFORMATION

The Protection of Personal Information (POPI) Act requires us to inform you how we use, disclose and destroy personal information we obtain from you. We are committed to protecting your privacy and will ensure that your personal information is used appropriately, transparently, securely and according to applicable law.

I, the undersigned, hereby consent to the following:

1. My personal information may be collected, processed, recorded, used and must be safeguarded during the rendering of financial services to me by Maptte (Pty) Ltd – FSP number 49733 (hereinafter referred to as the FSP).

2. The FSP may also add to my personal information, with information received from other product providers and third parties in order to offer a more comprehensive and appropriate service to me.

3. The FSP may verify, share and disclose my personal information to their product providers and third-parties whose services or products they use in order to adequately and appropriately render financial services to me.

4. The FSP may also collect and processes my personal information for the FSP's own marketing purposes to ensure their products and services remain applicable and appropriate.

5. The FSP is required by law to obtain and process information about you for the purposes of conducting Customer Due Diligence"(CDD) which includes enhanced due diligence. The purpose of CDD is to determine the risk that you may be engaged in money-laundering and/or terror-financing activities. We are required to obtain and process information about you in respect of the following:

- Your identity and that of any person whom you purport to represent, including your status as a prominent person as defined in the act;
- Your place of residence and/or registration of your business;
- Your status as defined by reference to sections 26A (i.e. whether you are a person against whom financial sanctions have been imposed) and section 28A (i.e. whether you are a person in respect of whom there is an absolute prohibition against doing business with);
- The nature and ownership/control structure of your business; and
- The nature of our products and services, how they relate to your requirements and how you use them.

In certain circumstances and in the course of our CDD activities, we may avail ourselves of detail available about you in the public domain as well as additional detail we require to verify some of the information we collect about you. These sources may include commercially and publicly available information with regards to references made about and by you in, including but not limited, the press and media including social media, law enforcement agencies such as Interpol and information collected and processed about you by credit bureax and similar agencies including the verification of bank account details in your name.

I hereby consent to and authorize the FSP and any agency lawfully appointed by us to obtain and process the information as described above as part of our duty in law. Furthermore, I understand that:

1. I have the right to access my personal information which the FSP holds.

2. I have the right to ask the FSP to update, correct or delete my personal information on reasonable grounds.

3. Once I object to the FSP processing my personal information, the FSP may no longer process my personal information, within reasonable parameters unless to conclude a transaction or outstanding business.

4. Should I wish to withdraw my consent to process my personal information, I must do so in writing, addressed to the FSP Information Officer.

5. Once I withdraw my consent for the FSP to process my personal information, I understand that the FSP is still obliged under other legislation to keep the information for 5 years after termination of the relationship between the FSP and myself.

6. The FSP may disclose my information where they have a duty or a right to disclose in terms of applicable legislation or where it may be necessary under any other law.

SIGNED AT……..ON THIS DAY……OF…….2021

C. **Proposed Email to obtain consent from clients for the processing and sharing of personal information:**

Dear Client,

<u>Consent to the Processing and Sharing of your Personal Information:</u>

We at Maptte, respect your constitutional right to privacy. We are committed to and bound by the terms and provisions of the Protection of Personal Information Act 4 of 2013 ("POPIA") regarding the processing (acquisition, usage, retention, transmission and deletion) and sharing of your personal information. The purpose of this email and the attached POPIA Notice and Consent Form is to obtain your consent in this regard, which will enable us at Maptte to lawfully process your personal information.

The attached POPIA Notice and Consent Form explains how we deals with your personal information and your rights in this regard. If you are in agreement, please provide your consent by either signing the attached POPIA Notice and Consent Form or provide your written consent by merely responding to this email (indicating that your email response serves as your written consent in this regard). It is important that you understand that your email response will be legally interpreted as follows -

"I hereby certify that my consent given via email for the processing and sharing of my personal information by Maptte , as explained in the attached Consent Notice, is as valid as my personal signature and I further certify that I have read, fully understand and accept all terms of the foregoing Notice".

If you would like more information in this regard you may also request our Privacy Notice which we will gladly provide.

Proposed POPIA Paragraph for use in Proposal, Quote, and Claim Forms as well as the Broker Appointment Templates:

<u>Protection of Personal Information</u>:

We at Maptte, respect your constitutional right to privacy. We are committed to and bound by the terms and provisions of the Protection of Personal Information Act 4 of 2013 ("POPI") regarding the acquisition, usage, retention, transmission, deletion and sharing of your personal information. We will check and validate

the information you provide through legal means. We have high level security measures in place to protect your personal information. Your personal information herein collected is for the primary purpose of providing you with insurance cover and for all other activities and processes incidental to and relevant to this purpose. Your information shall be kept confidential, however, we shall disclose it to certain third parties as required and other insurers for the specific purpose of insurance and to reduce and prevent any form of fraudulent activity. Sharing of information includes, but is not limited to, information sharing as arranged via the South African Insurance Association. You hereby give consent and fully understand the reason for Maptte to process, use, share and retain your personal information for its designated purpose and you confirm the accuracy of the information. You may request Maptte to amend, update, change or correct your personal information processed by us by sending a request to your Broker or our Deputy Information Officer, Maptte at email address. If your require more information on how we deal with your personal information and your rights in this regard we will gladly provide you with a copy of our Privacy Notice. Should you decide to cancel this insurance contract or business relationship you further consent to MaptteMaptte retaining the information in line with the legally permitted retention period, for statistical and reporting purposes only. Should you decide not to accept the proposal, the information collected, will be de-identified, on your request, and only used for statistical and research purposes.

Proposed POPIA Paragraph for use in Disclosure Template:

Disclosure Paragraph: Confidentiality and Privacy:

The FSP acknowledges that they will not, in the course of their agreement with a client or at any time, thereafter, process or disclose/share any confidential, private, or personal information obtained, except to the extent permitted by the client or required by applicable law. Your consent for the processing (which includes - collection, use, recording, organisation, storage, modification, transmission, distribution, and disclosure/sharing) of your personal information for the purposes indicated at the initial contact stage and subsequent compliance and other documentations are hereby obtained. Your consent will enable the FSP to process your personal information lawfully and transparently. Your rights in this regard are explained in our POPIA Manual (which includes our Privacy Notice and our PAIA Manual) and it is available on request.

Proposed Email Disclaimer with POPIA included:

Disclaimer:
The following terms shall apply to this e-mail communication, attachments and all subsequent e-mail communications and attachments, collectively referred to as the electronic message, which Maptte may send to you, the receiver. The information contained in this electronic message is confidential and may be legally privileged. It is intended solely for the use of the receiver (individual or entity) to whom Maptte has addressed the electronic message to, and others authorised by LVM to receive it. If you are not the intended receiver you are hereby notified that any disclosure, copying, distribution or taking action in reliance of the contents of this information is strictly prohibited and may be unlawful. If you are not the intended receiver of this e-mail (or such person's authorised representative), then please notify the sender of this e-mail immediately by return e-mail, facsimile or telephone and delete this message from your system. You may not print, store, forward or copy this message or any part thereof or disclose or cause information in this message to be disclosed to any other person. Maptte is not liable for the improper or incomplete transmission of the information contained in this electronic message, or for any delay in its receipt. Maptte is not liable for any harm or loss resulting from malicious software code or viruses in this e-mail or its attachments, including data corruption resulting there from. Any advice or information contained in this e-mail is subject also to any governing agreement between us. Only the Members of Maptte , is able to bind

the company contractually. No electronic communication including any data message such as an e-mail or SMS, sent or received will give rise to a binding legal transaction. Maptte shall not be liable if any variation is effected to any document or correspondence emailed unless that variation has been approved in writing and signed by an authorised company representative. Use of scanned versions of hand-rendered signatures to give the impression that an e-mail has been “signed” by the sender, is not permitted by Maptte and the inclusion of such a “signature” is of no additional force or effect. In accordance with the ECTA, an e-mail is only deemed to be received by Maptte once Maptte acknowledges receipt thereof. If this electronic message contains offensive, derogatory or defamatory statements or materials, it means the message has been sent outside the sender’s scope of employment with LVM and only the sender can be held liable in his/her personal capacity. Maptte respects your privacy and acknowledge that this e-mail will contain personal details, which may belong to you, others and/or to your company (personal information). By sending Maptte this email communication, you expressly give Maptte consent to process and further process the personal information which will be done in accordance with the Protection of Personal Information Act (4 of 2013) (POPIA), Maptte Privacy Notice and POPIA Policy (which is available on upon request) which sets out why Maptte needs the personal information, what Maptte will do with it, and with whom LVM will share it.
This e-mail disclaimer shall be governed by the law of South Africa.

D. Operator Assessment

Organization under assessment:	*Name of the organization*
Product(s) or service(s):	*Details of the specific offering from the organization that is being reviewed*
Date of Assessment:	*When the assessment started*
Assessor:	*Who is carrying out the assessment*
Assessor Comments:	*Explain any relevant circumstances that may affect the assessment outcome*

Organization Assessment

Registered Name:	*Official name e.g. name at Companies House, including type of organization*
Country of Registration:	*What nationality is the organization*
When Formed:	*When was it registered*
Approximate Size:	*Judge from website if necessary*
Contract Terms:	*Including length, renewal and termination provisions*
Applicable Law:	*From contract*
Certifications held:	*e.g. ISO/IEC 27001, Privacy Shield, ISO9001, Cyber Essentials*
Information Security Policy Available?:	*On website or available on request?*

Personal Data Compliance Assessment

Personal data held	*Describe the personal data that this supplier stores and/or processes on our behalf*
Business process(es) involved	*Name the business process(es) that require the use of this supplier to store or process personal data*
In which country or countries are the data stored and/or processed?	*Is the data guaranteed to remain in the stated country?*
Is the data encrypted and if so, to what standards?	*Is encryption used? Data centre protection*
What access controls are in place?	*How does the supplier control access to the personal data it holds on our behalf?*
Does the supplier share our personal data with any third parties and if so, who?	*Name third party's data are shared with, what data is involved and why. It may then be appropriate to assess these suppliers separately*

Result of Assessment

Assessment outcome:	*Raise any cause for concern e.g. storage outside the EU, lack of controls or inadequate information*
Actions arising:	*Describe what needs to be done to address any concerns and who will do the actions by when*
Date of assessment completion:	*Date (may be different to date of assessment)*
Assessor Comments:	*Any other relevant factors that should be considered*

E. Information Officer's Registration Form

NOTE: The personal information submitted herein shall be solely used for your registration with the Information Regulator ("Regulator").

All the information submitted herein shall be used for the purpose stated in section 55(2) of the Protection of Personal Information Act 4 of 2013 and the Promotion of Access to Information Act 2 of 2000, as mandated by law. This Information may be disclosed to the public. The Regulator undertakes to ensure that appropriate security controls measures are implemented to protect all the information to be submitted in this document.

Part A Information Officer	
Full Name of Information Officer	**Hector Makwakwa**
Designation	**Information officer**
Postal Address	**The Office zone** **24 Marie Rd** **Centurion 0157**
Physical Address	**The Office zone** **24 Marie Rd** **Centurion 0157**
Cellphone Number	**0670429723**
Landline Number	**010 0155765**
Fax Number	
Direct Email Address	**hector@maptte.co.za**
General Email Address	**info@maptte.co.za**
I consent to being contacted by the Regulator, requester or data subject at the above contact details or through my designated Deputy Information Officer(s), whose information is provided herein below.	

Part B Deputy Information Officer			
Person details of designated Deputy Information Officer(s)	Name	Name	Name
	Direct Landline	Direct Landline	Direct Landline
	Cellphone Number	Cellphone Number	Cellphone Number
	Email Address	Email Address	Email Address
Postal Address			
Physical Address			

Fax Number	
General Email Address	
I/We consent to being contacted by the Regulator, requester or data subject at the above contact details.	

Part C Body / Responsible Party				
Type of Body	Public Body		Private Body	
Full Name of the Body (Registered Name)				
Trading Name				
Registration No. if any				
Postal Address				
Physical Address				
Landline Number				
Fax Number				
Email Address				
Website				

Part D Declaration

I declare that the information contained herein is true, correct and accurate.

SIGNED **and** DATED **at _____ on this the _____ day of _____** 2023

_____
INFORMATION OFFICER

F. PAIA MANUAL

1. LIST OF ACRONYMS AND ABBREVIATIONS (*NB: please insert relevant applicable acronyms and abbreviations)*

1.1 “CEO” Chief Executive Officer

1.2 “DIO” Deputy Information Officer;

1.3 “IO“ Information Officer;

1.4 “Minister” Minister of Justice and Correctional Services;

1.5 “PAIA” Promotion of Access to Information Act No. 2 of 2000(as Amended;

1.6 “POPIA” Protection of Personal Information Act No.4 of 2013;

1.7 “Regulator” Information Regulator; and

1.8 “Republic” Republic of South Africa

2. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to-

2.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

2.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

2.3 know the description of the records of the body which are available in accordance with any other legislation;

2.4 access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

2.5 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

2.6 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

2.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;

2.8 know the recipients or categories of recipients to whom the personal information may be supplied;

2.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

2.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION

3.1. Chief Information Officer

Name: Hector Makwakwa
Tel: 010 015 5765
Email: hector@maptte.co.za
Fax number: Fax number

3.2. Deputy Information Officer (NB: if more than one Deputy Information Officer is designated, please provide the details of every Deputy Information Officer of the body designated in terms of section 17 (1) of PAIA.

Name: Name of the Deputy Information Officer
Tel: Work telephone numbers
Email: Email address
Fax Number: Fax number

3.3 Access to information general contacts

Email: Provide general email address for access to information

3.4 National or Head Office

Postal Address: Provide Postal Address

Physical Address: Provide physical address

Telephone: Provide general contact numbers for the organisation

Email: Provide general contact email address for the organisation

Website: Specify the website of the organisation, if any

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

4.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2. The Guide is available in each of the official languages and in braille.
4.3. The aforesaid Guide contains the description of-

4.3.1. the objects of PAIA and POPIA;

4.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of-

4.3.2.1. the Information Officer of every public body, and

4.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA ;

4.3.3. the manner and form of a request for-

4.3.3.1. access to a record of a public body contemplated in section 11 ; and

4.3.3.2. access to a record of a private body contemplated in section 50 ;

4.3.4. the assistance available from the IO of a public body in terms of PAIA and POPIA;

4.3.5. the assistance available from the Regulator in terms of PAIA and POPIA;

4.3.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-

4.3.6.1. an internal appeal;

4.3.6.2. a complaint to the Regulator; and

4.3.6.3. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

4.3.7. the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

4.3.8. the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.3.9. the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and

4.3.10. the regulations made in terms of section 92

4.4. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

4.5. The Guide can also be obtained-

4.5.1. upon request to the Information Officer;

4.5.2. from the website of the Regulator (https://www.justice.gov.za/inforeg/).

4.6 A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours-

4.6.1 (SPECIFY THE TWO OFFICIAL LANGUAGES)

5. CATEGORIES OF RECORDS OF THE (INSERT THE NAME OF THE BODY) WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

NB: Please specify the categories of records held by the body which are available without a person having to request access by completing Form C, types of the records and how the records can be accessed. These are mostly records that maybe available on the website and a person may download or request telephonically or by sending an email or a letter.

Below is an example of the table that can be used.

Category of records	Types of the Record	Available on Website	Available upon request
		X	X

6. DESCRIPTION OF THE RECORDS OF (INSERT THE NAME OF THE BODY) WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

NB: Please specify all the records which are created and available in accordance with any of the South African legislation. Below is an example of the table that can be used in describing the records and applicable legislation.

Category of Records	Applicable Legislation
Memorandum of incorporation	Companies Act 71 of 2008
PAIA Manual	Promotion of Access to Information Act 2 of 2000

7. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY THE (INSERT THE NAME OF THE BODY)

NB: Describe the subjects (i.e. Finance, SCM or HR), in respect of which the body holds records and the categories of records held on each subject. Below is an example of the table that can be used. .

Subjects on which the body holds records	Categories of records
Strategic Documents, Plans, Proposals	Annual Reports, Strategic Plan, Annual Performance Plan.
Human Resources	- HR policies and procedures - Advertised posts - Employees records

8. PROCESSING OF PERSONAL INFORMATION

8.1 Purpose of Processing Personal Information

NB: Describe the purpose or reasons for processing personal information in your organisation.

8.2 Description of the categories of Data Subjects and of the information or categories of information relating thereto

NB: Specify the categories of data subjects in respect of whom the body processes personal information and the nature or categories of the personal information being processed.

Below is the template that can be used to set out the categories of data subjects and the description of the nature or categories of the personal information to be processed. Note that the nature or categories of the personal information is dependent on the purpose of the body in performing its functions or services. .

Categories of Data Subjects	Personal Information that may be processed
Customers / Clients	name, address, registration numbers or identity numbers, employment status and bank details
Service Providers	names, registration number, vat numbers, address, trade secrets and bank details
Employees	address, qualifications, gender and race

8.3 The recipients or categories of recipients to whom the personal information may be supplied

NB: Specify the person or category of persons to whom the body may disseminate personal information. Below is an example of the category of personal information which may be disseminated and the recipient or category of recipients of the personal information

Category of personal information	**Recipients or Categories of Recipients to whom the personal information may be supplied**
Identity number and names, for criminal checks	South African Police Services

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Qualifications, for qualification verifications	South African Qualifications Authority
Credit and payment history, for credit information	Credit Bureaus

8.4 Planned transborder flows of personal information

NB: Indicate if the body has planned transborder flows of personal information. For example, some personal information may be stored in the cloud outside the Republic. Please specify the country in which personal information will be stored and categories of personal information.

8.5 General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information

NB: Specify the nature of the security safeguards to be implemented or under implementation to ensure the confidentiality and integrity of the personal information under the care of the body. This may, for example, include Data Encryption; Anti-virus and Anti-malware Solutions.

9. AVAILABILITY OF THE MANUAL

9.1 A copy of the Manual is available-

9.1.1 on (specify the website), if any;

9.1.2 head office of the (name of the body) for public inspection during normal business hours;

9.1.3 to any person upon request and upon the payment of a reasonable prescribed fee; and

9.1.4 to the Information Regulator upon request.

9.2 A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

F. Data Protection

1. Data protection principles

The FSP is committed to processing data in accordance with its responsibilities under the Protection of Personal Information Act.

Condition 1 – 8 under Protection of Personal Information Act requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. General provisions

a. This policy applies to all personal data processed by the MAPTTE.
b. The Responsible Person shall take responsibility for the MAPTTE's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The NAME shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the NAME shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the NAME shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the NAME must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
b. The NAME shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the NAME's systems.

5. Data minimisation

a. The NAME shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. [Add considerations relevant to the NAME's particular systems]

6. Accuracy

a. The NAME shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. [Add considerations relevant to the NAME's particular systems]

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the NAME shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The NAME shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the NAME shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

H.RECORDS MANAGEMENT

The FSP has the responsibility to facilitate, store and archive certain documentation, records and other forms of information for specific periods

DEFINITIONS

"Record" refers to recorded information, regardless of format or medium, which has been created, received, used, accessed and maintained by FSP Name as evidence and information in pursuance of its legal obligations or in the transaction of business. Included are e-mails, records in electronic form and records other than correspondence. Business record has a corresponding meaning.

"Disposal" refers to the actions taken with regard to records as a consequence of the expiration of their retention periods. Disposal may involve one of the following activities:

Transfer to a storage facility or records centre; Transfer of permanent records to archives; or Destruction of ephemeral records.

"Destruction" refers to the physical disposal of documents of no further value by shredding, pulping, etc.

Ensure that important business records are easily located and readily accessible to FSP Name and promote constitutional values such as efficiency, transparency and accountability;

Ensure that FSP Name disposes of (destruction/transfer to archives) and deletes (destroy) unnecessary records in accordance to referring South African legislation and operational requirements;

Maintains the physical and electronic security of records; and retains records in such a manner that their admissibility and/or evidential weight is not compromised.

Employees leaving FSP Name or changing positions within FSP Name are to leave all records for their successors.

Operational responsibility for records management rests with the key individual/records manager . The FSP is the custodian of the Records Management Policy.

ROLES AND RESPONSIBILITIES OF EMPLOYEES

Record keeping is an essential role of all employees. Every employee is responsible for making and keeping such records as may be necessary to fully and accurately record the functions, transactions, operations, decisions, administration and management of FSP Name (Pty) Ltd.

FILING OF BUSINESS RECORDS

Records (both paper and electronic) are classified as confidential. Refer to our E-mail Usage Policy.

Only approved paper-based filing systems and electronic folder systems may be used.

A record is a register, file, electronic recording or a written comment of information about a transaction or event.

Records need to be kept in a secure environment, which may not be on your premises, but would be easily accessible to a client or the Registrar on request. A FSP must (unless the Registrar exempts him in any way) maintain records for a minimum period of five years.

The Records of all verbal and written communication relating to any financial service rendered to a client or product accepted by the client

Records must be kept for a period of five years after the termination of that service or product.

ACCESS TO RECORDS

Access to records by employees and third parties will be dealt with in accordance with the PAIA Manual.
Inactive records located in the archive may only be accessed via senior management and may only be accessed, copied and used upon the written authorisation of the manager.
A record in the custody of the person must remain "accessible" to authorized individuals until final destruction.

CONFIDENTIALITY AND NON-DISCLOSURE

Employees may not disclose the contents of any record to any person unless such disclosure is permitted in terms of the employees'. job description, contract of employment or upon written authorization from senior management in consultation with the key individual. Each employee employed by FSP has signed a non disclosure agreement and has a confidentiality clause in their employment contracts.

STORAGE MEDIA AND FILE FORMATS

When selecting storage media and file formats for electronic records, due consideration must be given to the security, integrity, and accessibility requirements of the records

RECORD DISPOSAL

The procedure for disposing of paper and electronic records must be adhered to at all times.

INTEGRITY

All records will be identified, classified, retained, stored and protected in such a manner that their integrity is not compromised. In this regard, the key individual and the senior management ensure that processes and applicable technology are implemented to safeguard the integrity of records across the record lifecycle.

COMPLIANCE WITH THE RECORDS MANAGEMENT POLICY

Any employee that fails and/or refuses to discharge any duties detailed in this Policy and the associated procedures and instructions will be required to explain such failure and/or refusal in a disciplinary hearing. Disciplinary actions may result in dismissal. A claim of ignorance as to the existence and/or application of this Policy shall not be a ground for justification of non-compliance.
Any uncertainty as to the provisions of this Policy or any duty detailed herein will be directed to the key individual/senior management.
Adherence to the Records Management Policy will be annually reviewed.

ELECTRONIC BACKUP AND RECOVERY TESTING PROCEDURE

The following procedure for electronic backup has been adopted by the FSP.

All client documentation including correspondence, application forms and minuted paperwork is scanned using a digital scanner and stored in a readable electronic format such as PDF. '

Once scanned and converted to digital format, the documents are filed according to client name and surname in a specified central storage location.

All electronic client folders stored centrally are easily accessible via a computer interface inside the offices of the financial practice.

Centrally stored client folders and company emails are backed up on an external tape drive or equivalent removable storage on a monthly basis. The removable storage is stored off-site in a secure and fire-proof environment.

Proof of backup/synchronization to the removable storage is confirmed by the appointed staff member.

Recovery testing is done on a quarterly basis

I. Incident Response Plan

Introduction

Maintaining the privacy and protection of customers' and employees' personal information is a risk management issue for all organizations.

The increase in identity theft is a concern for all of us. Business systems and processes are increasingly more complex and sophisticated and more and more personal information continues to be collected. Laws and regulations continue to place requirements on businesses for the protection of personal information.

Incident Response Plan

An Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

Incident Response Team

An Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Information Security Officer will coordinate these investigations.

The Incident Response Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents.

Incident Response Team Members

Each of the following areas will have a primary and alternate member:

- Information Officer (ISO)
- Chief Information Officer (CIO)
- Management

Incident Response Team Roles and Responsibilities

Information Officer

- Determines the nature and scope of the incident
- Contacts qualified information security specialists for advice as needed
- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Provides proper training on incident handling
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate

- Prepares a written summary of the incident and corrective action taken

Chief Information Officer

- Central point of contact for all computer incidents
- Notifies IO to activate computer incident response team

Incident Response Team Notification

The Information Officer (IO) will be the central point of contact for reporting computer incidents or intrusions. The Chief Information Officer will notify the IO.

All computer security incidents must be reported to the IO. A preliminary analysis of the incident will take place by the IO and CIO and that will determine whether Incident Response Team activation is appropriate.

Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of Personal Information
- Denial of Service / Distributed Denial of Service
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak

Breach of Personal Information - Overview

This Incident Response Plan outlines the steps our business will take upon discovery of unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a customer or employee of our business.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the organization collects about an individual is likely to be considered personal information if it can be attributed to an individual.

For our purposes, personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- ID Number
- Driver's license number or Identification Card number
- Banking account number, credit or debit card number* with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
- Home address or e-mail address
- Medical or health information

Definitions of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Requirements

Data owners must identify and document all systems and processes that store or utilize personal information on individuals. Documentation must contain system name, device name, file name, location, database administrator and system administrator (primary and secondary contacts for each). The business area and the IT development group must maintain the contact list of database and system administrators.

Likewise, all authorized users who access or utilize personal information on individuals should be identified and documented. Documentation must contain user name, department, device name (i.e., workstation or server), file name, location, and system administrator (primary and secondary contacts).

Data Owner Responsibilities

Data owners responsible for personal information play an active role in the discovery and reporting of any breach or suspected breach of information on an individual. In addition, they will serve as a liaison between the company and any third party involved with a privacy breach affecting the organization's data.

All data owners must report any suspected or confirmed breach of personal information on individuals to the IO immediately upon discovery. This includes notification received from any third party service providers or other business partners with whom the organization shares personal information on individuals. The IO will notify the CIO and data owners whenever a breach or suspected breach of personal information on individuals affects their business area.

The CISO will determine whether the breach or suspected breach is serious enough to warrant full incident response plan activation (See "Incident Response" section.) The data owner will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the IO, CIO or other Incident Response Team members throughout the investigation.

Location Manager Responsibilities

Location managers are responsible for ensuring all employees in their buisness unit are aware of policies and procedures for protecting personal information.

If a breach or suspected breach of personal information occurs in their location, the location manager must notify the IO immediately and open an incident report. (See "Incident Response")

Note: Education and awareness communication will be directed to all employees informing them of the proper procedures for reporting a suspected breach of personal information on an individual.

When Notification Is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.

- An intruder has broken into database(s) that contain personal information on an individual.

- Computer equipment such as a workstation, laptop, hard drive, or other electronic media containing personal information on an individual has been lost or stolen.

- A department or unit has not properly disposed of records containing personal information on an individual.

- A third party service provider has experienced any of the incidents above, affecting the organization's data containing personal information.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the organization can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

- The organization is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.

- The organization determines that personal information on an individual was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.

- An intruder accessed files that contain only individuals' names and addresses.

- A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.

Incident Response – Breach of Personal Information

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

1. The IO will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual.

   IO contact information: Maptte-Maptte

2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the IO will open a Incident Request.

1. When notified by the IO, the CIO performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.

2. Informs management and the IO that a possible privacy breach has been reported and provides them an overview of the situation.

3. Contacts the individual who reported the problem.

4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).

5. Reviews the preliminary details with the IO.

6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted.

7. Notify the Public Relations Department of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.

8. The IO is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.

9. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.

10. Contact appropriate Incident Response Team members and First-Level Escalation members.

11. Identify and contact the appropriate Data Owner affected by the breach. In coordination with the management, IO and Data Owner, determine additional notification requirements (e.g., Human Resources, external parties).

12. If the breach occurred at a third party location, determine if a legal contract exists. Work with the Legal Department, Information Privacy Office and Data Owner to review contract terms and determine next course of action.

13. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.

14. Determine the type of personal information that is at risk, including but not limited to:

    Name, Address, Social Security Number, Account number, Cardholder name, Cardholder address, Medical and Health Information

15. If personal information is involved, have the Data Owner determine who might be affected. Coordinate next steps with the IO.

16. Determine if an intruder has exported, or deleted any personal information data.

17. Determine where and how the breach occurred.

    - Identify the source of compromise, and the timeframe involved.
    - Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.
    - Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.

18. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

    - Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
    - Do not access or alter the compromised system.
    - Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
    - Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.

19. Monitor systems and the network for signs of continued intruder access.

20. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

21. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the company.

Customer Database Owners

IT Customer Database Contacts	Office Phone	Pager	E-Mail
Primary: Alternate:			
Data Owner Contacts	Office Phone	Pager	E-Mail
Primary: Alternate:			

Notification Steps

1. If the IT Customer Database group or Data Owners hear of or identifies a privacy breach, contact the IO to ensure that the CIO and other primary contacts are notified.

2. The IT Customer Database group and Data Owner will assist the CIO as needed in the investigation.

3. IT Customer Database contact notifies the IT Contractor Liaison (if warranted).

Process Steps

1. Monitor access to customer database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).

2. Identify individuals whose information may have been compromised. An assumption could be “all” if an entire table or file was compromised.

3. Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.

4. Upon request from the CIO, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

Human Resources

Contacts	Office Phone	Pager	E-Mail
Primary: Alternate: David Mamedzi	010 015 5765		david@maptte.co.za

1. If notified of a privacy breach affecting employee personal information, open an incident request with the IO to activate the Incident Response Plan for suspected privacy breach.

2. When notified that the privacy breach incident response plan has been activated for a breach of information on an individual, perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.

3. Work with the IO, management and and business area to identify the extent of the breach.

4. If appropriate, notify the business area that a breach has been reported and is under investigation.

5. Work with the business area to ensure there is no further exposure to privacy breaches.

Location Manager

Contacts	Office Phone	Pager	E-Mail
Primary: Alternate: Mitchell Murirwa	010 015 5765		info@maptte.co.za

1. If the Location/Branch Manager becomes aware of or identifies a privacy breach, contact the IO to ensure that the CIO and other primary contacts are notified.

2. The Location Branch Manager will secure the area of the breached information (e.g. computer room, data center, records room).

3. The Location/Branch Manager will assist the CIO as needed in the investigation.

4. The Location/Branch Manager will keep the CIO updated on appropriate investigation information gathered.