2. Policy: Information Transfer

2.1. INTRODUCTION

This Policy regulates the transfer of information within and from and to the Company. Where the information being transferred consists of Personal Information, the provisions of POPIA will apply to the processing of information by or on behalf of the Company.

2.2. PURPOSE

There are many occasions when information is transferred between different departments of the Company, and between the Company and third-party service providers, clients, customers, and the like. This transfer of information is affected by a wide variety of media and methods, in both electronic and paper format. In every transfer of information, there is a risk that the information in question may be lost, misappropriated, or accidentally disclosed. Where the information in question is Personal Information, or confidential, sensitive, critical, or proprietary information of the Company, the risk to the Company increases significantly.

The Company has a duty of care in handling information. It is essential that the transfer of information is performed in a way that adequately protects such information. It is always the responsibility of the sender of information to assess the risks involved in the transfer of information and to ensure that controls are in place to mitigate such risks. This Policy outlines the responsibilities attached to, and the minimum-security requirements, for the transfer of information, including Personal Information, and Confidential Information.

This Policy applies to all areas in the Company where Personal Information, and Confidential Information is created, accessed, processed, updated, stored, maintained, or managed.

This Policy applies to all employees, contractors, visitors, and other persons (Users) authorised to access and use the Company's systems who are involved in the transfer of information.

2.3. POLICY

Electronic communication channels

The Company's information may be exchanged through the electronic communication channels, such as email. New data channels must be approved by the Information Officer prior to being implemented. The Information Officer's approval will set out the type of communication allowed, and controls pertaining to the use of the data channel. Public information may be made available to the public. All information meant for internal use only, may only be transferred to parties that are authorised by the Company to receive such information, and that are bound contractually not to disclose such information.

Where the information is classified as either Personal Information, or Confidential Information, the Company should ensure that such information is transferred in a secure manner and that only certain secure channels are used:

- Email may be used to transfer Personal Information, and Confidential Information only when such information has been sufficiently password protected or properly encrypted:
- A file transfer method may be used to transfer Personal Information, or Confidential Information only when a secure file transfer protocol channel is used.
- Portable Media (such as CDs, DVDs, USB drives and memory cards) may be used to transfer Personal Information, and Confidential Information only when such information on the device in question is properly password protected or encrypted.
- Telephonic communication, fax transmission, mobile voice or SMS communication, and social media may not be used to transfer or disclose Personal Information, or Confidential Information.

Non-electronic communication channels

The Company's information may be exchanged through the non-electronic communication channels outlined below.

Where the information is classified as either Personal Information, and Confidential Information, the guidelines set out below should be used to ensure that such information is transferred in a secure manner:

- Registered or normal post may not be used to transfer Personal Information, and Confidential Information.
- Letters delivered by hand may be used to transfer Personal Information, or Confidential Information only when the sender of such information ensures that the party receiving the information is properly identified and authorised to receive such information.

2.4. RESPONSIBILITIES OF THE SENDER AND RECEIVER OF INFORMATION

The sender's responsibilities for transferring Personal Information, and Confidential Information are:

- Assessing the information to be sent and ensuring that it is in line with the guidelines set out in this Policy.
- Ensuring that the identity of the receiver is known that such receiver is authorised to receive the information.
- Ensuring that the transfer of information is formally confirmed and documented.
- Ensuring that the information is sent and tracked in an appropriate manner to ensure compliance with this Policy.

The person receiving Personal Information, and Confidential Information is responsible for ensuring that:

- The information received is information that they have a right to receive.
- They fully disclose their identity.

2.5. RELATIONSHIP WITH EXTERNAL PARTIES

Before exchanging any information with any person or party outside of the Company, an agreement must be concluded between the Company and third-party. Such agreement must comply with POPIA and must contain at least the following clauses:

- Method of identification of the third-party.
- Confirmations or warranties regarding authorisation to access information.
- Technical standards and appropriate Data Channels for the transfer of information.
- Labelling and handling of Personal Information, and Confidential Information.
- Warranties from the third-party regarding compliance with POPIA and all other relevant privacy laws.
- Obligations on the third-party to safeguard the security of the information in question.
- Indemnities in favour of the Company in the event of a breach by the third-party of POPIA or the agreement itself.
- Protections for the Company's intellectual property rights.
- Incident responses and what must be done in the event of security breaches.

2.6. TRANSBORDER PERSONAL INFORMATION FLOW

Technological developments in the field of information, computers and communications are leading to significant structural changes in the economy of South Africa. Flows of computerised data and information are an important consequence of technological advances and are playing an increasing role in national economies. With the growing economic interdependence of countries, these flows acquire an international dimension, known as Transborder Personal Information Flows.

Transborder transfer of information is subject to RICA (Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002), FICA (Financial Intelligence Centre Act, 2001), ECTA (Electronic Communications and Transactions Act, 2002) and the POPI Act, 2013.

The Company may not transfer Personal Information about a data subject to a third-party who is in a foreign country unless adequate levels of protection are provided by:

- The Law of the country.
- Binding Corporate Rules of the third-party to which Personal Information is provided.
- A binding Agreement between the Company and the third-party in the foreign country.
- The Law, Corporate Rules or Binding Agreement must uphold the principles of reasonable processing, like the Conditions of Lawful Processing in Chapter 3 of POPIA.
- The data subject consents to the transfer (*Refer to Annexure A*).

In view of the above, Chapter 3 of POPIA acknowledges that:

- Computerised data and information now circulate freely on an international scale.
- Recognises the diversity of participants in Transborder Personal Information Flows, such as commercial and non-commercial organisations, individuals, and governments.
- Recognising the wide variety of computerised data and information, traded, or exchanged across national borders.
- Recognises the growing importance of Transborder Personal Information Flows and the benefits that can be derived from transborder data flows.
- Recognises the national policies which affect Transborder Personal Information Flows.
- Is aware of the social and economic benefits resulting from access to a variety of sources of information and of efficient and effective information services.
- Recognises that member countries have a common interest in facilitating Transborder Personal Information Flows, and in reconciling different Policy objectives in this field.

The POPI Act has the intention to:

- Promote access to data and information and related services and avoid the creation of barriers to the international exchange of data and information.
- Seek transparency in Regulations and Policies relating to information, computer and communications services affecting Transborder Personal Information Flows.
- Develop common approaches for dealing with issues related to Transborder Personal Information Flows and develop harmonised solutions.
- Consider possible implications for other countries when dealing with issues related to Transborder Personal Information Flows.

2.7. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

2.8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

2.9. POLICY AWARENESS AND UPDATE

Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

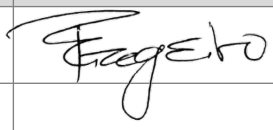
Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

2.10. INTERNAL DOCUMENT APPROVAL

Information Officer Name	Signature	Date
Mrs Paula Gageiro		23 June 2021

2.12. DOCUMENT VERSION CONTROL

Version	Date	Summary of Changes