enquiries@theinfocompany.co.za

PRIVACY POLICY

Prepared in terms of the Protection of Personal Information Act of 2013

DUELCO INVESTMENTS 24 (PTY) LTD t/a THE INFO COMPANY (PTY) LTD

Registration Number: 2001/000492/07

DATE OF COMPILATION: AUGUST 2026

TABLE OF CONTENTS

CONTENTS

1. OBJECTIVE

1.1 Duelco Investments 24 (Pty) Ltd trading as The Info Company ("**the Info Company**") is committed to collecting, storing and processing the personal information of our clients ("subscribers") in a manner compliant with the Protection of Personal Information Act 4 of 2013 ("POPIA") and the Promotion of Access to Information Act 2 of 2000 ("PAIA").

1.2 Insofar as it is required in terms of POPIA, we will always obtain the written consent of our clients before processing your personal information in any way.

2 DEFINITIONS

2.1 "**PAIA**" means Promotion of Access to Information Act No. 2 of 2000 (as amended);

2.2 "**POPIA**" means the Protection of Personal Information Act No.4 of 2013;

2.3 "**Personal Information**" means "information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person";

2.4 "**The Info Company**" is a private company incorporated in terms of the laws of the Republic of South Africa under registration number: 2001/000492/07;

2.5 "**Data Subject**" means "the person to whom personal information relates." In the context of The Info Company, the Data Subjects are the clients, otherwise known as the subscribers;

2.6 "**Responsible Party**" means The Info Company;

2.7 "**Consent**" means "voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information";

2.8 "**Processing**" means "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information";

2.9 "**Record"** means "any recorded information, regardless of form or medium, in the possession or under the control of a responsible party, whether or not it was created by a responsible party and regardless of when it came into existence";

2.10 "**Regulator**" means "the Information Regulator established in terms of Section 39."

3 GENERAL

3.1 The Info Company undertakes to treat all client information as strictly confidential, insofar as it is required by South African data protection legislation and insofar as the same information is not already in the public domain or made available as such with the express consent of the client.

3.2 The Info Company will not request, gather or store any personal information from or regarding a client, unless this is done for business purposes and takes place with the full knowledge and consent of the client concerned. The information collected and processed is only used for the specified purpose for which it was intended, as set out at the time of procurement.

3.3 We undertake to provide access to our clients, upon request, to their own records, in terms of the provisions of POPIA, and where sufficient proof of identity has been shown upon such request.

4 INFORMATION OFFICER

The details of our Information Officer are as follows:

Name: Hendrik Christoffel Viljoen

Tel: 073 160 6846 (SA) or 00264 81142 1966 (Namibia)

Email: enquiries@theinfocompany.co.za

5 INCIDENT MANAGEMENT PROCECSS

5.1 The Info Company acknowledges that the Processing of Personal Information by electronic or other means carries inherent security risks.

5.2 While The Info Company implements appropriate and reasonable technical measures to maintain the integrity and confidentiality of the Personal Information in its possession, and while the majority of the information stored and processed by us is in any event in the public domain / accessible to the public, the possibility of unauthorised access, disclosure, or loss due to security breaches cannot be entirely excluded.

5.3 The processing of data, particularly by electronic means, is always accompanied by a certain element of risk. Although we do everything in our power to safeguard the integrity of the personal information entrusted to us, security breaches are still a possibility.

5.4 Where we have become aware of a data security breach / have reasonable grounds to believe that there has been a data security breach, this will be reported to the Information Regulator, as well as the data subject concerned, as soon as reasonably possible after becoming aware of the compromise / possible compromise, and following an internal assessment of the potential breach occurred. We will provide enough information to allow the data subject to take action against any potential consequences.

5.5 Should The Info Company become aware of, or have reasonable grounds to suspect, a security breach involving personal information, the incident will be assessed and managed by the Information Officer. Appropriate steps will be taken to contain the breach, assess the impact, and implement remedial measures where required.

6 EMPLOYEE AWARENESS AND COMPLIANCE

6.1 The Info Company does not currently employ any personnel. Accordingly, the employee awareness and training measures set out in this section will become applicable should personnel be appointed in the future.

6.2 Upon the appointment of any employee, The Info Company will ensure, as part of the employee's induction and as a condition of employment, that the employee is made aware of their obligations under this Policy and POPIA, including their responsibilities relating to the lawful processing, security, and confidentiality of Personal Information.

6.3 The Info Company will provide appropriate POPIA and information security awareness training to employees and will promote ongoing awareness of information security risks.

6.4 The Info Company will ensure that employees are informed of the procedures for reporting actual or suspected personal information security incidents and of their obligation to comply with the Info Company's information security and data protection policies.

7 DOCUMENTS CONTAINING PERSONAL INFORMATION

7.1 **Electronic Information Systems**

7.1.1 The Info Company stores Personal Information electronically using a password-protected laptop and secure cloud-based storage. Access to the laptop and the information stored on it is restricted to the authorised individuals responsible for the company's operations.
7.1.2 The laptop password and all other login credentials are confidential and are known only to the authorised users. Passwords may not be shared with or disclosed to any unauthorised person.

7.1.3 Access to the Info Company's cloud-based storage and any systems containing personal information is restricted to authorised users only and is protected by appropriate authentication measures.

7.1.4 Should authorised users cease to be associated with the Info Company or no longer require access, all access rights to the laptop, cloud-based systems, email accounts, and any repositories containing personal information will be revoked without undue delay, and passwords will be changed where necessary.

8 REMOTE COMPUTERS

8.1 Where potential, future authorised personnel will be required to work remotely from a location other than the Info Company's registered premises, access to our cloud-based systems and personal information will be permitted only through secure, password-protected devices and accounts.

8.2 Potential, future authorised personnel will need to obtain prior approval before removing our laptop or any other company-owned device from the premises. Such devices must be always kept secure and may not be used by any unauthorised person.

8.3 While working remotely, potential, future authorised personnel will be responsible for taking reasonable steps to protect personal information from unauthorised access, disclosure, loss, theft, or misuse, and will have to ensure that confidential information is not accessible to third parties

9 ACCESS CONTROLS

9.1 Access to personal information processed by the Info Company is restricted to the director and other authorised persons only. The Info Company implements reasonable physical, technical and organisational measures to prevent unauthorised access to personal information.

9.2 Access to devices, systems and records containing personal information is controlled and limited to persons who require such access for legitimate business purposes.

9.3 Where any third party or service provider requires access to personal information, such access will be limited to what is necessary for the relevant purpose and subject to appropriate confidentiality and security obligations.

10 RISK ANALYSIS

The Information Officer conducts an annual review of the company's risk analysis and data security safeguards, including the measures implemented to protect the company's physical, digital, operational, and administrative security.

11 SUB-CONTRACTORS

11.1 Where the Info Company appoints external service providers, contractors, or operators who may have access to personal information processed by us, such access will be limited to what is necessary for the services being provided.

11.2 The Info Company will take reasonable steps to verify, where appropriate, that service providers handling personal information have adequate security measures and procedures in place to protect such information.

12 BACK-UP SUPPORT

The Info Company maintains electronic backups of information stored on its laptops and other authorised devices through its Microsoft cloud-based account.

13 UPDATING OF THE MANUAL

The Information Officer of the Info Company will on a regular basis update this manual.

Issued by

Hendrik Christoffel Viljoen

CEO and Information Officer