TRIPLE ADVANCED INVESTMENTS 51 (PTY) LTD

2010/018513/07

Information Classification Policy

1. DOCUMENT VERSION CONTROL

Version Number	Date	Created by	Comments
1	17 June 2021	G.L. Esterhuizen	

2. SENSITIVITY OF INFORMATION

2.1 Information:

2.1.1 must be handled with due care and in accordance with authorised procedures;

2.1.2 must be made available only to people within the organisation who have a legitimate 'need to-know' to fulfil their official duties or contractual responsibilities; and

2.1.3 must only be processed and released in accordance with applicable Policy directives and Legislative requirements.

2.2 The information classification policy sets the minimum requirements for the classification of Information to ensure the appropriate degree of data protection required.

3. SCOPE

3.1 The policy is intended to address classification of information across all delivery and storage mechanism and to apply to both electronic and non-electronic stored information and is intended for the use by all managers and employees within the organisation.

4. REFERENCE DOCUMENTS

- IT Security Policy
- Information Privacy Policy
- Personal Information Retention Policy
- Personal Information Processing Policy

5. CLASSIFICATION OF INFORMATION

5.1 The level of confidentiality is calculated based on the following criteria:

5.1.1 Sensitivity of information for the organisation; and

5.1.2 Legislative and Contractual obligations.

5.2 All Information is allocated a security classification as follows:

5.2.1 Confidentiality level 1 - Public Information

Information that is freely available or accessible to the public and in instances where the information is made public by the Organisation, it cannot harm the Organisation. Examples of Public documents/records include: Marketing materials authorised for public release, published annual reports, Internet web pages, external vacancy notices etc.

5.2.2 Confidentiality level 2 - Internal Information

Information which is available to all employees and selected third parties. Unauthorised access to information would not be in breach of a legislative requirement but may cause minor damage and/or inconvenience to the Organisation. Examples of Internal use Information documents/records are: Policies and Procedures, departmental memos, phone and email directories, internal transaction data, operational reports and contracts.

5.2.3 Confidentiality level 3 - Restricted Information

Information that is made available or accessible to a specific group of employees and authorised third parties. Unauthorised access to information may considerably damage the business and/or the reputation of the Organisation. Examples of Restricted Information are: Policies, Procedures and legal opinions specifically marked as restricted, , vendor information, security investigation reports, and most accounting records

5.2.4 Confidentiality level 4 - Confidential Information

Information that is made available only to a specific group of employees and authorised third parties. Unauthorised access to the information would be in breach of a legislative requirement and may cause catastrophic damage to the business and/or to the reputation of the Organisation. Examples of Confidential Information are: Personal Information as defined by the Protection of Personal Information Act 4 of 2013, Credit Information as defined by the National Credit Act 34 of 2005, Passwords and PIN codes and other highly sensitive or valuable proprietary information.

5.3 The Classification of information and the allocation of the minimum-security control requirements in respect of each level of classification must be determined and implemented as

soon as possible by the Information Officer and Deputy Information Officers and reviewed regularly.

6. COMPLIANCE

6.1 Any employee that fails and/or refuses to discharge any duties detailed in this Policy and the associated procedures and instruction will be in breach of the Policy. Any uncertainty as to the provisions of this Policy or any duty detailed herein may be directed to the Information Officer and/or Deputy Information Officers.

G.L. Esterhuizen

Information Officer