SANANBIL Capital Ltd.
Confidentiality Policy

February 2024
Version 1.0

1. Introduction

SANABIL Capital Ltd. (ex Oryx Capital Ltd.) is a Securities Dealer with a license number SD173 regulated by the Seychelles Financial Services Authority (FSA) and a registration number 8434986-1 (The "Company").

The company is operating under the Securities Act of 2007, and its amendments. The Company will provide those securities and / or perform those investment activities in relation to those securities, as specified in its authorization. This is conditional that it holds such an authorization from the FSA.

It is important that the Company protects and safeguards person-identifiable and confidential consumer information that it gathers, creates processes and discloses. This policy sets out the requirements place on the Company when sharing information.

The Company's Confidentiality Policy is prepared pursuant to Part VII of the Financial Consumer Protection Act of 2022 on the Protection of Consumer Data and Confidentiality.

2. Scope

This policy aims to ensure protection on non-public consumer information, especially for the expectation as to the manner in which the Company, its employees, agents or to other relevant parties acting on its behalf hold, treat, and use information received from actual or potential clients who intend to or partake in the products or services offered.

The scope of this policy includes the protection of the confidentiality, integrity and availability of consumer information.

This policy and all standards apply to all protected personal information of the Company's consumers in any form as defined below under "Information Classification".

3. Information Classification

Non-public consumer data includes any information which in not publicly known. Classification is used to promote proper controls for safeguarding and confidentiality of consumer information. Regardless of the classification, the integrity and accuracy of all classifications of information must be protected.

The Classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail in includes. Information recorded in several formats (e.g. source document, electronic record, report) must have the same classification regardless of the format.

The following levels are to be used when classifying information.

Protected Information

Protected information comprises of all information created or received by the Company. Unauthorized or improper disclosure, modification, or destruction of this information could violate applicable laws and regulations, result in civil and / or criminal penalties, and cause serious damage to Company's clients.

Confidential Information

Confidential information is very important and considered highly sensitive material that is not classified as protected information. This information is private or otherwise sensitive in nature and mush be restricted to those with a legitimate business need for access.

Examples of Confidential Information may include: personal system access passwords and information file encryption keys. Unauthorized disclosure of this information to anyone without a business need for access may violate applicable laws and regulations, or may cause significant problems for the Company's clients. Decisions about the provision of access to this information must always be cleared through the information owner.

Internal Information

Internal information is intended for unrestricted use within the Company, and in some cases within affiliated organizations such as the Company's business partners. This type of information is already widely-distributed within the Company, or it could also distributed within the organization without advance permission from the information owner.

Examples of internal information may include: personal directories, most internal electronic mail messages. Any information that is no explicitly classified as protection information, confidential information and / or public information will, by default, be classified as internal information. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

Public Information

Public information has been specifically approved for public release by a designated authority with the Company. This information may be disclosed outside of the Company.

4. Purposes of Collecting Non-Public Consumer Data

The Company obtains non-public consumer data in a number of ways through clients' use of its services including the use of Company's websites, applications, the account opening applications, demo sign up forms, webinar sign up forms, subscribing to news updates and from the information provided in the course of ongoing customer service communications. The Company may also collect this information from third parties such as through publicly available sources.

The personal data provided to the Company is used to verify contact information and identity. The Company also uses personal data to register clients, open and configure trading accounts and issue activation codes and passwords. Be providing contact information, the client helps us to improve our services and promptly communicate the availability of additional services, features, and promotions we may be offering.

5. Discolosure Procedure of Non-Public Consumer Data

The Company adopts security practices and procedures to safeguard non-public consumer data. Firstly, the Company shall not disclose any of its clients' confidential information to a third party, except:

(a) To the extent that it is required to do so pursuant to any applicable laws, rules and/or regulations; and / or
(b) If there is a duty to the public to disclose; and/or
(c) If the Company's legitimate business interests require disclosure; and/or
(d) At consumer's request or upon his consent or to the persons described in this Policy.

The Company will endeavor to make such disclosures on a 'need-to-know' basis, unless otherwise instructed by a regulatory authority. Under such circumstances, the Company will notify the third party regarding the confidential nature of any such information.

Depending on the products and services concerned and the relevant restrictions on sensitive data, personal information may be disclosed to:

- potential successors in title to our business;
- third party consultants, contractors or other service providers who may access non-public consumer data when providing services (including IT support services) to us;
- any organization or person acting on consumer's behalf to whom the consumer requests us to provide information, including financial advisors, brokers, solicitors or accountants;
- third parties where it is necessary to process a transaction or provide services requested by the consumer;
- to a Trade Repository or similar;
- Banks (upon request of additional information following payments that clients made);
- credit providers, courts, tribunals and regulatory authorities in response to legal and regulatory requests or other government agencies, as agreed or authorized by law;
- auditors or contractors or other advisers auditing, assisting with or advising on any of our business purposes, in any jurisdiction where we operate;
- at consumer's request or upon his consent.

Secondly, the Company follows mechanisms to control access to Protected Information, Confidential Information and Internal Information. Access is granted on a ''need to know'' basis and must be authorized by the immediate supervisor and application owner with the assistance of the Chief Technology Officer. Any of the following methods are acceptable for proving access under this policy:

I. Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The ''external'' factors might include time of day, location of the user, strength of user authentication, etc.;
II. Role-based access: An alternative to traditional access control models (e.g. discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to as organization's

structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role;

III. User-based access: A security mechanism needs to grant users of a system access based upon the identity of the user.

IV. Identification/Authentication: Unique user identification (user id) and authentication is required for all systems to maintain or access Protected Information, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id;

V. At least one of the following authentication methods must be implemented:

1. Strictly controlled passwords (see Exhibit A- Password Control Standards);
2. Biometric identification; and/or
3. Tokens in conjunction with a PIN.

- The user must secure his/her authentication control (e.g. password token) such that it is known only to that user and possibly a designated security manager;
- An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes);
- The user must log off or secure the system when leaving it.

6. How We Obtain Consumer's Consent

Where the Company uses of consumer's personal information, it requires his consent. Such consent will be provided in accordance with the express written terms which govern our business relationship (which are available on our website(s) as amended from time to time), or any other contract we may have entered into with the client or as set out in our communication with the client from time to time.

By submitting any personal information (including, without limitation, account details) to the Company, the consumer consent to the use of information as set out in this Statement. We reserve the right to amend or modify this Statement and if we do so, we will post the changes on the Website.

If we rely on consumer's consent as our legal basis for holding and processing non-public consumer data, consumers have the right to withdraw that consent at any time by contacting us, using the contact details set out in this policy.

7. Storage of non-public consumer data and retention period

Safeguarding the privacy of non-public consumer data is of utmost importance to us, whether the consumer interacts with the Company, personally, by phone, by mail, over the internet or any other electronic medium. We will hold personal information, for as long as we have a business relationship with the consumer, in a combination of secure computer storage facilities and paper-based files and other records. We take the necessary measures to protect the personal information we hold from misuse, loss, unauthorized access, modification or disclosure.

When we consider that non-public consumer data is no longer necessary for the purpose for which it was collected, we will remove any details or we will securely destroy the records. However, we may need to maintain records for a significant period of time. For example, we are subject to certain anti-money laundering laws which require us to retain the following, for a period of seven (7) years after our business relationship has ended:

- a copy of the documents we used in order to comply with our customer due diligence obligations;
- supporting evidence and records of transactions with the consumer and his relationship with us.

Also, the personal information we hold in the form of a recorded communication, by telephone, electronically, in person or otherwise, will be held in line with local regulatory requirements (i.e. 7 years after our business relationship has ended). Where the client has opted out of receiving marketing communications, we will hold non-public consumer details on our suppression list so that we know he does not want to receive these communications. We may keep non-public consumer data for longer than 7 years if we cannot delete it for legal, regulatory or technical reasons.

8. Amendments

We may, at any time and at our discretion, vary this, Policy. We will notify our clients, if we amend this Confidentiality Policy, by contacting them through the contact details provided to us. Any amended Confidentiality Policy is effective once we notify of the change.

9. How to contact us

If you have any questions regarding this Policy, wish to access or change your information, or if you have any questions about security on our website, you may email us at info@sanabilcapital.com.