DATA POLICY

***FOR*:** **LOUISE TONKIN INCORPORATED**

["the Company"]

1 TABLE OF CONTENTS

2 INTRODUCTION

2.1 Employees who are granted the privilege of access to data must adhere to strict guidelines regarding the appropriate use of this resource. Users who violate the provisions are subject to disciplinary action in terms of the Company's disciplinary codes and procedures. Access to data shall not be used for any illegal or unlawful purposes, i.e. abuse involving criminal offences such as fraud and threats. Users must note that access to data is strictly limited to activities in direct relation to official business, and their duties and job description.

2.2 This policy provides the procedures for the use of any data within the Company and will ensure that all policies remain current and relevant. It will, therefore, be necessary from time to time to modify and amend some sections of the policies and procedures, or to add new procedures.

3 VALUES AND PRINCIPLES

3.1 The Company is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic data and personal information of the institution to ensure that regulatory, operational and contractual requirements are met.

3.2 The Company ensures that information is accessible only to those authorised to have access, while safeguarding the accuracy and completeness of information when processing and archiving data and personal information.

4 OBJECTIVES

4.1 The purpose of this policy is to establish guidelines and responsibilities for the use of data and personal information in the Company. The policy includes the protocol for regulating the use of the Company's internet facilities, as well as general control and associated services, to ensure business continuity, minimise business damage and maximise return on business opportunities with a view to protecting the reliability and completeness of all information.

4.2 This policy provides guidelines for the following:

4.2.1 Compliance with requirements for confidentiality, integrity and availability of information of the Company's employees, clients, suppliers, customers and other stakeholders;

4.2.2 Establishing controls for protecting the Company's information and information systems against theft, abuse and other forms of harm and loss;

4.2.3 Motivating administrators and employees to meet their responsibility in terms of ownership of and knowledge about information security in order to minimise the risk of security incidents;

4.2.4 Ensuring that the Company is capable of continuing operations even in the event of major security incidents;

4.2.5 General communication practices, social media management and confidentiality of information;

4.2.6 Managing the risk of usage and guiding users as to what is acceptable;

4.2.7 The use of Company-owned or sponsored personal computers, laptops, phones, fax machines, notebooks, printers, related hardware and any Company software;

4.2.8 Access to and disclosure of electronic mail messages sent or received by employees, and storage and printing of confidential information.

5 INTERPRETATION

5.1 **"Biometrics"** means a technique of personal identification based on physical, physiological or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

5.2 "**Business Operations"** means internal personnel and financial information, vendor names and other vendor information (including vendor characteristics, services and agreements), purchasing and internal cost information, internal services and operational manuals, and the manner and methods of conducting the client's business.

5.3 **"Confidential Information"** means–

5.3.1 any information or data relating to the client (even if not marked as being confidential, restricted, secret, proprietary or any similar designation), in whatever format and whether recorded or not (and if recorded, whether recorded in writing, on any electronic medium or otherwise), which by its nature or content is identifiable as, or could reasonably be expected to be, confidential and/or proprietary to the client;

5.3.2 information relating to the client's existing and future strategic objectives and existing and future business plans and corporate opportunities, trade secrets, technical information, techniques, know-how, operating methods and procedures;

5.3.3 details of costs, sources of materials and customer lists (whether actual or potential) and other information relating to the pricing, price lists and purchasing policies of existing and prospective customers and suppliers of the clients.

5.3.4 computer data, programs and source codes, whether relating to the client or a third party; and

5.3.5 intellectual property of the client and/or in respect of which it has rights of use or possession.

5.4 **"Consent"** means any voluntary, specific and informed expression agreeing to the processing of personal information.

5.1 **"Constitution"** means the Constitution of the Republic of South Africa, 1996 (Act No. 1088 of 1996).

5.2 **"Customers"** means names of customers and their representatives, contracts and their contents and parties, customer services, data provided by customers and the type, quantity and specifications of products and services purchased, leased, licensed or received by clients of the client.

5.3 **"Data"** means any information relating to a **"data subject"** which was obtained as a result of a legal agreement between the **"responsible party"** and "**data subject"**. The information may be held in hardcopy form (e.g. as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically.

5.4 **"Data Subject"** means the "**person**" to whom personal information relates, including a third party or any natural person or legal Company whose personal and/or business details were made known to the **"responsible party"**.

5.5 **"Company"** means the LOUISE TONKIN INCOPRPRATED with registration number 2013/034352/21.

5.9 **"Electronic communication''** means any text, voice, sound or image message sent over an electronic communications network and which is stored in the network or on the recipient's terminal equipment until it is collected by the recipient.

5.10 **"Filing system''** means any structured set of **"personal information"**, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

5.11 "Information" means any "confidential information" or "personal information".

5.12 **"Information System"** means the process of, and tools for, storing, managing, using and gathering of **"data**" and communications in an organisation.

5.13 **"Information Officer"** means the **"person"** acting on behalf of the client and discharging the duties and responsibilities assigned to the Head of the Private Body in terms of the Promotion of Access to Information Act, 2 of 2000 (PAIA).

5.14 **"Marketing and Development Operations"** means marketing and development plans, price and cost data, price and fee amounts, pricing and billing policies, quoting procedures, marketing techniques and methods of obtaining business, forecasts and forecast assumptions and volumes, and future plans and potential strategies of the client which have been or are being discussed.

5.15 **"Personal information"** means information of an identifiable, living or deceased natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to–

5.15.1 race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth or death of a **"person"**;

5.15.2 education, medical, financial, criminal or employment history;

5.15.3 the biometric information of the **"person"**;

5.15.4 ID number, symbol, e-mail address, physical address, telephone number or other particular assignment or unique allocation to a **"person"**;

5.15.5 private or confidential correspondence;

5.15.6 the personal views, opinions or preferences of the **"person"**;

5.15.7 a name, if it appears together with other Personal information or if disclosure of the name itself would reveal Personal information about the **"person"**; and

5.15.8 the views or opinions of another individual about a **"person"**.

5.16 **"Personal Requester"** means a **"requester**" seeking access to a **"record"** containing "**personal information"** about the "**requester"** himself / herself.

5.17 **"Processing"** means any operation or activity, whether or not by automatic means, including–

5.17.1 collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

5.17.2 dissemination by means of transmission, distribution or making available in any form;

5.17.3 merging, linking, erasure or destruction.

5.18 **"Record"** means any recorded information, regardless of form or medium, including writing, electronic information, label, marketing, image, film, map, graph, drawing or tape which is in the possession or under the control of the client, irrespective of whether it was created by the client and regardless of when it came into existence.

5.19 **"Request"** means a request for access to a **"record"** or information of "**the Company"** and **"the client"**.

5.20 **"Responsible party"** means a person who obtained or is in possession or determines the purpose and means of processing personal information (typically, but not always, the collector of information), and includes **"the Company"** and **"the client".**

5.21 **"Third Party",** in relation to a "request" for access, means any "person", excluding "the client" or a "personal requester".

6 SCOPE

6.1 This policy applies to all employees of the Company (temporary and permanent) as well as independent contractors who work on the premises of the Company or who have access to the data of the Company.

6.2 All employees are required to fully understand and comply with the policy as set out in this document.

6.3 The Company reserves the right to monitor user activities, including phone and internet records, for compliance with information security principles.

6.4 The scope, type and purpose of the collection, processing and/or use of personal data undertaken by Employees for the Company are specified in this agreement.

6.5 Every other transfer to a third party requires the prior consent of the Company, which must be given when the special requirements of the applicable provisions of the Protection of Personal Information Act (POPI) are met.

7 GENERAL GUIDELINES

7.1 In addition, employees' observation of the provisions of the respectively applicable provisions of POPI entails the following duties:

7.1.2 Written appointment – insofar as this is required by law – of a data protection officer who can carry out his/her tasks in compliance with the respectively applicable provisions of POPI. The contact information of the data protection officer shall be made available for the purposes of direct contact.

7.1.3 Observation of data confidentiality pursuant to the respectively applicable provisions of POPI: All persons who have access to the personal data of the Company by virtue of the mandate are obliged to maintain confidentiality of the data and must be instructed in the special data protection duties arising from this mandate and the existing instruction and purpose commitment.

7.1.4 The implementation and observation of all technical and organisational measures necessary for this mandate in compliance with the respectively applicable provisions of POPI.

7.1.5 Immediate notification of the Company with regard to the control procedures and measures of the supervisory authority pursuant to the respectively applicable provisions of POPI. This also applies should a competent authority investigate Employees in accordance with the respectively applicable provisions of POPI.

7.1.6 Job control by means of regular checks by Employees with regard to the execution or fulfilment of the mandate, in particular the observation and, where applicable, the necessary adaptation of provisions and measures for the performance of the mandate.

7.1.7 Verifiability of the technical and organisational measures implemented *vis-à-vis* the Company. In this respect employees are free to choose an adequate means of verification. The Company may request, at its own cost, specific attestations, reports or report excerpts of independent bodies (e.g. auditors, audits, data protection officer, IT security departments, data protection auditor, quality auditor) or appropriate certification by an IT security or data protection audit (e.g. pursuant to BSI basic protection). Employees are free to comply with such a request.

7.1.8 Overall the measures to be implemented relate to organisational control, physical access control, system access control, data access control, transmission control, job control, availability control and separation requirement, and provide guidelines and rules with regard to the type of data exchange / data provision, / the type / circumstances of processing / data storage and the type / circumstances of output / data transmission.

7.1.9 The technical and organisational measures are subject to technical progress and further development. In this respect employees are permitted to implement alternative adequate and appropriate measures which must not fall short of the safety level of the specified measures. Significant and material changes must be documented. On request, employees are obliged to provide the Company with the information stipulated in the respectively applicable provisions of POPI.

8 SUB-CONTRACTORS

8.1 The Company hereby agrees to the use of the abovementioned sub-contractors' services. Should further sub-contractors be used for the processing or use of the Company's personal data, this is permitted without the permission of the Company, provided the following requirements are fulfilled:

8.1.1 Employees are obliged to compile the contractual agreements with the sub-contractor in such a way that they comply with the data protection provisions agreed between employees and the Company.

8.1.2 The requirements of the respectively applicable provisions of POPI must be observed during execution of the sub-mandate and, in particular, the Company must be granted control and examination rights *vis-à-vis* the sub-contractor in compliance with the respectively applicable provisions of POPI. The sub-contractors mandated by employees are in turn themselves entitled to mandate sub-contractors provided that they observe the aforementioned

requirements.

8.1.3 Such third-party services that employees make use of as ancillary services for supporting the execution of the mandate are not considered sub-mandates pursuant to this provision. These include, for example, telecommunication services, maintenance and user services, cleaning staff, auditors, or the disposal of data media. However, employees are obliged to ensure adequate protection and safety of the Company's data, even in the case of ancillary services mandated with third parties, and to conclude lawful contractual agreements and implement control measures.

9 THE COMPANY'S POWER TO GIVE INSTRUCTIONS

9.1 Data shall be handled exclusively within the framework of this policy and on the instruction of the Company. The Company reserves the right, within the framework of this policy, to give instructions with regard to the type, scope and procedures of the data processing and to specify more closely by means of individual instructions. Changes in the subject matter of the processing and changes in procedures must be agreed mutually and documented. Employees may not give information to any third parties or to the person concerned without the prior written approval of the Company.

9.2 Verbal instructions relating to any aspect regulated by this policy shall be confirmed by the Company without delay in writing or per email (in text form).

9.3 In compliance with the respectively applicable provisions of POPI, employees are obliged to inform the Company without delay if they believe an instruction infringes upon any data protection provisions. Employees are entitled to defer performance of the relevant instruction until such time as this has been confirmed or modified by the responsible person at the Company.

10 ERASURE OF DATA AND RETURN OF DATA MEDIA

10.1 Employees are obliged to hand over, or by prior agreement to destroy in compliance with data protection provisions, all documents, compiled results of processing and use and stored data that came into their possession. The same applies to test and rejected material. The log of the erasure must be submitted on request.

10.2 Documentation that serves to verify mandated and proper data processing must be stored by employees in accordance with the respective storage periods. In order to disencumber themselves, employees may hand over such documentation to the Company.

10.3 Employees are obliged to implement technical and organisational measures provided for below for protection of the Company's data stored on their servers or on the servers of affiliated companies.

11 CONFIDENTIALITY IN GENERAL

11.1 All information shall be considered confidential. Confidentiality protects assets from unauthorised disclosure. At no stage during the employment relationship may an employee disclose any information to any person inside or outside the Company. Any information that is shared, irrespective of form, except where it is permitted, shall lead to disciplinary action.

11.2 Employees should never disclose any confidential information about Company, fellow employees, consultants, clients, customers, vendors, suppliers or competitors.

11.3 Employees should maintain the confidentiality of Company trade secrets and information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. This also includes internal reports, policies, procedures or other internal business-related confidential communications.

11.4 Employees are obliged to report any breach or possible or suspected breach of this policy immediately to their supervisor or manager.

12 TRAINING

12.1 Information security training should be presented once a year for all employees working with information.

12.2 The information officer appointed in the organisation has the main responsibility of ensuring that training courses are held for each employee of the Company.

13 THIS POLICY SHOULD BE READ IN CONJUNCTION WITH THE FOLLOWING POLICIES:

13.1 Information Technology (IT) Policy

13.2 Physical Access and Information Security Policy

13.3 Record and Archiving Management Policy

13.4 Remote Working from Home Policy