| | |
|---|---|
| Document Title | The Cape Town Stock Exchange POPIA Policy |
| Version | 2 |
| Publishing Date | **03 June 2021** |
| Last Review Date | **28 October 2022** |
| Frequency of Review | **Annually or as and when required** |
| Next Review Date | **28 October 2023** |
| Plan Owner | **Compliance Officer** |
| Responsible Business Unit | **Compliance** |

**DOCUMENT DRAFT HISTORY**

| DATE | VERSION | STATUS | REVIEWERS | ACTION/COMMENT |
|---|---|---|---|---|
| 3 June 2021 | V1 | Draft | COO | None |
| 11 June 2021 | V1.1 | Draft | Executive | |
| 28 October 2022 | V1.2 | Draft | Executive | |

**CHANGE PROTOCOL**

- Any requirement for change or clarification should be addressed to the Document Owner, as defined in thispolicy, who will log the issue in the Issue Log.
- Compliance shall maintain the Issues Log.
- Issues must be collected via the Issues Log until the regular policy review date, at which point all identified issueswith respect to this policy must be considered and addressed as part of the policy review and update process.
- Once the review has been finalised, all Divisional Heads must sign off on the changes made to this policy beforeit may be submitted to the Board of Directors for approval.

## TABLE OF CONTENTS

## 1. PURPOSE

1.1 The purpose of this document is to clearly set out how CTSE will meet its RegulatoryObligations to promote and ensure the Protection or Personal Information.

## 2 INTRODUCTION

2.1 The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

2.2 POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

2.3 Through the provision of quality services, CTSE is necessarily involved in the collection, useand disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

2.4 A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

2.5 Given the importance of privacy, CTSE is committed to effectively managing personal information in accordance with POPIA's provisions and All CTSE Employees are responsible for complying with this Policy.

## 3 DEFINITIONS AND INTERPRETATION

### 3.1 Definitions

In this Policy, the following words have the following meanings:

| | |
|---|---|
| CTSE | The Cape Town Stock Exchange Pty Ltd ("CTSE") (formerly 4 Africa Exchange Pty Ltd) (registration number: 2013/031754/07), a private company duly incorporated in accordance with the laws of South Africa and licensed as an exchange under the FMA,including any subsidiaries or associates; |
| Board | the duly elected and constituted Board of directors of CTSE; |
| Biometric | technique of personal identification that isbased on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition; |
| CEO | CTSE's chief executive officer or managing directorappointed by CTSE from time to time; |
| CFO | the chief financial officer or financial director of CTSE, who is also a Senior Manager, appointed from time to time; |
| Client | any person to whom an Authorised User or Participant provides Securities Services and includesany person that acts as an agent for another in relation to those services, in which case it will include the agent or exclude the other person if the contractual arrangement between the parties indicates this to be the intention; |
| Consent | Means any voluntary, specific, and informed expression of will in terms of which permission isgiven for the processing of personal information; |
| COO | the chief operating officer of CTSE's, who is also a Senior Manager, appointed from time to time; |

| | |
|---|---|
| CO | the Compliance Officer of CTSE, also a Senior Manager, appointed from time to time; |
| Data Subject | the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the organisation with products or other goods; |
| De-Identify | to delete any information that identifies adata subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject; |
| Deputy Information Officer | any senior employee appointed by the CTSE Information Officer; |
| Direct Marketing | Means to approach a data subject, either in person or by mail or electronic communication, for the director indirect purpose of:<br>i. Promoting or offering to supply, in the ordinary course of business, any goods orservices to the data subject; or<br>ii. Requesting the data subject to donate any kind for any reason; |
| Employee | a director, officer, manager, agent or staff member; |
| Exchange | the exchange operated by CTSE in terms of theExchange Licence; |
| Exchange Licence | the licence granted to CTSE by the FSCA to operate the Exchange in terms of the FMA; |
| Executive Committee | the Executive Committee of CTSE which is required to report to the Board, consisting of, *inter alia*, the following Senior Managers:<br>i. the CEO;<br>ii. the CFO;<br>iii. the COO;<br>iv. the CO;<br>v. the CRO;<br>vi. the Head of IRD and<br>vii. Head of Registry. |
| FICA | the Financial Intelligence Centre Act, 28 of 2001; |
| Filing System | any structured set of personal information, whether centralised, decentralised or dispersed on afunctional or geographical basis, which is accessible according to specific criteria in electronic or paper- based format; |
| FMA | the Financial Markets Act 19 of 2012 and any subordinate legislation including any regulations, notices or directives issued by the FSCA in terms ofthat Act; |
| FSCA | the Financial Sector Conduct Authority or its successor organisation established under theFinancial Sector Regulation Act, 2017; |
| Information Officer | the Information Officer is responsible for ensuring the organisation's compliance with POPIA. Where noInformation Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties. |

| | |
|---|---|
| | Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer. |
| Issuer | has the meaning ascribed to it in the FMA; |
| Operator | an operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third- party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause. |
| Participant | has the meaning ascribed to it in the FMA; |
| Personal Information | Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:<br>i. 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 of a person;<br>ii. information relating to the education or the medical, financial, criminal or employment history of the person;<br>iii. any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;<br>iv. the Biometric information of the person;<br>v. the personal opinions, views or preferences of the person;<br>vi. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;<br>vii. the views or opinions of another individual about the person;<br>viii. the personal opinions, views or preferences of the person;<br>ix. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person. |
| Processing | the act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal informationand includes:<br>i. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultationor use;<br>ii. dissemination by means of transmission, distribution or making available in any other form; or<br>iii. merging, linking, as well as any restriction, degradation, erasure or destruction of information. |

| | |
|---|---|
| Record | any recorded information, regardless of formor medium, including:<br>i. writing on any material;<br>ii. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;<br>iii. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;<br>iv. book, map, plan, graph or drawing;<br>v. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced. |
| Re-Identify | in relation to personal information of a data subject,means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject; |
| Regulatory Obligations | any obligation or duty that CTSE has in terms of the FMA, any FSCA directive or the Exchange Licence; |
| Responsible Party | the responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processingthe personal information. In this case, the organisation is the responsible party. |
| Senior Managers | has the same meaning ascribed to it in the FMA andmay include the COO, CFO and or the Head of IRD as the context indicates; |
| South Africa | the Republic of South Africa as constituted from timeto time; and |
| Unique Identifier | any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party. |

3.2 Where any term is defined within the context of any particular section in this POPIA Policy, the term so defined, unless it is clear from the section in question that the term so defined has limited application to the relevant section, will bear the same meaning as ascribed to it for all purposes in terms of this Policy, even though that term has not been defined in this interpretation section.

3.3 Where figures are referred to in numerals and in words, if there is any conflict between the two, the words will prevail.

3.4 Where in terms of this Policy, CEO permission is required, and it is the CEO himself who seeks to conduct the activity covered by this Policy, two other members of the Board shall be asked to give their permission for the CEO to act in accordance with this Policy.

## 4 PURPOSE

4.1 The purpose of this policy is to protect CTSE from the compliance risks associated with the protection of personal information which includes:

4.1.1 **Breaches of confidentiality.**
For instance, CTSE could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.

4.1.2 **Failing to offer choice.**
For instance, all data subjects should be free to choose how and for what purpose CTSE uses information relating to them.

4.1.3 **Reputational damage**.
For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by CTSE.

4.2 This policy demonstrates CTSE's commitment to protecting the privacy rights of data subjects in the following manner:

4.2.1 through stating desired behaviour and directing compliance with the provisions of POPIA and best practice;

4.2.2 by developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information;

4.2.3 by creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of CTSE;

4.2.4 by assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers to protect the interests of CTSE and data subjects;

4.2.5 by raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

## 5 ORGANISATIONAL SCOPE

5.1 This policy and its guiding principles apply to:

5.1.1 CTSE's governing body

5.1.2 all branches, business units and divisions of CTSE and its subsidiaries;

5.1.3 all employees and volunteers; and

5.1.4 all contractors, suppliers and other persons acting on behalf of CTSE.

5.2 The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA is activated in any situation where there is:

5.2.1 a processing of personal information entered into a recordby or for a responsible person who is domiciled in South Africa.

5.3 POPIA does not apply where the processing of personal information:

5.3.1 is concluded during purely personal or household activities; and

5.3.2 where the personal information has been de-identified.

## 6 RIGHTS OF DATA SUBJECTS

6.1 Where appropriate, CTSE will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. CTSE will ensure that it gives effect to the following six rights:

6.1.1 **The right to access Personal information**:

CTSE recognises that a data subject has the right to establish whether CTSE holds personal information related to him, her or it is including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under Annexure A.

6.1.2 **The right to have Personal information corrected or deleted:**

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where CTSE is no longer authorised or required by law or regulation to retain the personal information.

6.1.3 **The right to object to the processing of Personal information:**

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

In such circumstances, CTSE will give due consideration to the request and the requirements of POPIA. CTSE may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

6.1.4 **The right to object to Direct Marketing:**

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

6.1.5 **The right to complain to the Information Regulator:**

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a POPIA Complaint Form can be found in Annexure B.

6.1.6 **The right to be informed:**

The data subject has the right to be notified that his, her or its personal information is being collected by CTSE. The data subject also has the right to be notified in any situation where CTSE has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

## 7 GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of CTSE will always be subjected to , and act in accordance with the following guiding principles:

7.1 **Accountability:**

Failing to comply with POPIA could potentially damage CTSE's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

CTSE will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, CTSE will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

7.2 **Processing Limitation:**

CTSE will ensure that personal information under its control is processed:

7.2.1 in a fair, lawful and non-excessive manner;

7.2.2 only with the informed consent of the data subject; and

7.2.3 only for a specifically defined purpose.

CTSE will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, CTSE will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

CTSE will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's businessand be provided with the reasons for doing so.

An example of a POPI Notice and Consent Form can be found under Annexure C.

7.3 **Purpose Specification:**

All CTSE's business units and operations must be informed by the principle of transparency. CTSE will process personal information only for specific, explicitly defined and legitimate reasons. CTSE will inform data subjects of these reasons prior to collectingor recording the data subject's personal information.

**7.4 Further processing limitations:**

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where CTSE seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and wherethis secondary purpose is not compatible with the original purpose, CTSE will first obtain additional consent from the data subject.

**7.5 Information quality:**

CTSE will take reasonable steps to ensure that all personal information collected is complete,accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the organisationwill put into ensuring its accuracy.

Where personal information is collected or received from third parties, CTSE will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directlywith the data subject or by way of independent sources.

7.6 **Open Communication:**

CTSE will take reasonable steps to ensure that data subjects are notified that their personal information is being collected including the purpose for whichit is being collected and processed.

CTSE will ensure that it establishes and maintains a “contact us” facility, for instance via itswebsite or through an electronic helpdesk, for data subjects who want to:

7.6.1 enquire whether the organisation holds related personal information; or

7.6.2 request access to related personal information; or

7.6.3 request the organisation to update or correct related personal information; or

7.6.4 make a complaint concerning the processing of personal information.

7.7 **Security safeguards:**

CTSE will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification, and or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as financial information or credit card details, the greater the security required.

CTSE will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network.

CTSE will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

CTSE's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in CTSE's employment contracts can be found under Annexure D.

An example of an "SLA Confidentiality Clause" for inclusion in CTSE's service level agreements can be found under Annexure E.

7.8 **Data Subject participation:**

A data subject may request the correction or deletion of his, her or its personal information held by the organisation. CTSE will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information. Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

## 8 INFORMATION OFFICERS

8.1 CTSE will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer. CTSE's Information Officer is responsible for ensuring compliance with POPIA.

8.2 There are no legal requirements under POPIA for CTSE to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.

8.3 Where no Information Officer is appointed, the head of CTSE will assume the role of the Information Officer. Consideration will be given on an annual basis to the re- appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers

8.4 Once appointed, CTSE will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An example of an "Information Officer Appointment Letter" can be found under Annexure F.

## 9 SPECIFIC DUTIES AND RESPONSIBILITIES:

### 9.1 Governing body:

CTSE 's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

9.1.1 CTSE appoints an Information Officer, and where necessary, a Deputy Information Officer.

9.1.2 All persons responsible for the processing of personal information on behalf of the organisation:
9.1.2.1 are appropriately trained and supervised to do so,
9.1.2.2 understand that they are contractually obligated to protect the personal information they encounter, and
9.1.2.3 are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

9.1.3 Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

9.1.4 The scheduling of a periodic POPIA Audit to accurately assess and review the ways in which CTSE collects, holds, uses, shares, discloses, destroys and processes personal information.

### 9.2 Information Officer:

CTSE's Information Officer is responsible for:

9.2.1 Taking steps to ensure CTSE's reasonable compliance with the provision of POPIA.

9.2.2 Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

9.2.3 Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing CTSE's information protection procedures and related policies.

9.2.4 Ensuring that POPIA Audits are scheduled and conducted on a regular basis.

9.2.5 Ensuring that CTSE makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the organisation. For instance, maintaining a "contact us" facility on CTSE's website.

9.2.6 Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of CTSE's employment contracts and other service level agreements.

9.2.7 Encouraging compliance with the conditions required for the lawful processing of personal information.

9.2.8 Ensuring that employees and other persons acting on behalf of CTSE are fully aware of the risks associated with the processing of personal information and that they remain informed about CTSE's security controls.

9.2.9 Organising and overseeing the awareness training of employees and other individuals

involved in the processing of personal information on behalf of CTSE.

9.2.10 Addressing employees' POPIA related questions.

9.2.11 Addressing all POPIA related requests and complaints made by CTSE's datasubjects.

9.2.12 Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer(s) will assist the Information Officer in performing his or her duties.

9.3 **Chief Operations Officer:**

CTSE's Chief Operations Officer will ensure that:

9.3.1 Ensuring that CTSE's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.

9.3.2 Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computingservices.

9.3.3 Ensuring that servers containing personal information are sited in a secure location, away from the general office space.

9.3.4 Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.

9.3.5 Ensuring that all back-ups containing personal information are protected fromunauthorised access, accidental deletion and malicious hacking attempts.

9.3.6 Ensuring that personal information being transferred electronically is encrypted.

9.3.7 Ensuring that all servers and computers containing personal information areprotected by a firewall and the latest security software.

9.3.8 Performing regular IT audits to ensure that the security of the organisation 'shardware and software systems are functioning properly.

9.3.9 Performing regular IT audits to verify whether electronically stored personalinformation has been accessed or acquired by any unauthorised persons.

9.3.10 Performing a proper due diligence review prior to contracting with operators orany other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

9.4 **Chief Executive Officer:**

CTSE's Chief Executive Officer is responsible for:

9.4.1 Approving and maintaining the protection of personal information statements anddisclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.

9.4.2 Addressing any personal information protection queries from journalists or mediaoutlets.

9.4.3 Where necessary, working with persons acting on behalf of the organisation toensure that any outsourced marketing initiatives comply with POPIA.

9.5 **Employees and other persons acting on behalf of CTSE:**

Employees and other persons acting on behalf of CTSE will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of CTSE are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of CTSE may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within CTSE or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of CTSE will only process personal informationwhere:

9.5.1 The data subject, or a competent person where the data subject is a child,consents to the processing: or

9.5.2 The processing is necessary to carry out actions for the conclusion orperformance of a contract to which the data subject is a party; or

9.5.3 The processing complies with an obligation imposed by law on the responsibleparty; or

9.5.4 The processing protects a legitimate interest of the data subject; or

9.5.5 The processing is necessary for pursuing the legitimate interests of theorganisation or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

9.5.6 Clearly understands why and for what purpose his, her or its personalinformation is being collected; and

9.5.7 Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of CTSE will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, CTSE will keep a voice recording of the data subject's consenting instances where transactions are concluded telephonically or via electronic video feed.

9.6 Consent to process a data subject’s personal information will be obtained directly from thedata subject, except where:

9.6.1 The personal information is made public, or

9.6.2 Where valid consent has been given to a third party, or

9.6.3 The information is necessary for effective law-enforcement.

9.7 Employees and other persons acting on behalf of CTSE will under no circumstances:

9.7.1 Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks orduties.

9.7.2 Save copies of personal information directly to their own private computers,laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and

updated from the organisation's central database or a dedicated server.

9.7.3 Share personal information informally. Personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.

9.7.4 Transfer personal information outside of South Africa without the express permission from the Information Officer.

9.8 Employees and other persons acting on behalf of CTSE are responsible for:

9.8.1 Keeping all personal information secure, bytaking sensible precautions and following the guidelines outlined within this policy.

9.8.2 Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore becreated.

9.8.3 Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending orsharing of personal information to or with authorised external persons.

9.8.4 Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not beshared with unauthorised persons.

9.8.5 Ensuring that their computer screens and other devices are switched off orlocked when not in use or when away from their desks.

9.8.6 Ensuring that where personal information is stored on removable storage mediassuch as external drives, CDs or DVDs that these are kept locked away securely when not being used.

9.8.7 Ensuring that where personal information is stored on paper, that such hardcopy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

9.8.8 Ensuring that where personal information has been printed out, that the paperprintouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.

9.8.9 Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update theinformation accordingly.

9.8.10 Taking reasonable steps to ensure that personal information is stored only for aslong as it is needed or required in terms of the purpose for which it was originallycollected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

9.8.11 Undergoing POPIA Awareness training from time to time.

Where an employee, or a person acting on behalf of CTSE, becomes aware or suspiciousof any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

## 10 POPIA AUDIT

10.1 CTSE's Information Officer will schedule periodic POPIA Audits. The purpose of a POPIA audit isto:

10.1.1 Identify the processes used to collect, record, store, disseminate and destroy personal information.

10.1.2 Determine the flow of personal information throughout CTSE. For instance, CTSE's various business units, divisions, branches and other associated organisations.

10.1.3 Redefine the purpose for gathering and processing personal information.

10.1.4 Ensure that the processing parameters are still adequately limited.

10.1.5 Ensure that new data subjects are made aware of the processing of theirpersonal information.

10.1.6 Re-establish the rationale for any further processing where information isreceived via a third party.

10.1.7 Verify the quality and security of personal information.

10.1.8 Monitor the extend of compliance with POPIA and this policy.

10.1.9 Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.

In performing the POPIA Audit, Information or Deputy Officers will liaise with line managers in order to identify areas within CTSE's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

## 11 REQUEST TO ACCESS PERSONAL INFORMATION

11.1 Data subjects have the right to:

11.1.1 Request what personal information the organisation holds about them and why.

11.1.2 Request access to their personal information.

11.1.3 Be informed how to keep their personal information up to date.

11.2 Access to information requests can be made by email, addressed to the InformationOfficer. The Information Officer will provide the data subject with a "Personal Information Request Form".
Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requestswill be processed and considered against the organisation's PAIA Policy.
The Information Officer will process all requests within a reasonable time.

## 12 POPIA COMPLAINTS PROCEDURE

12.1 Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. CTSE takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

12.1.1 POPIA complaints must be submitted to the organisation in writing. Where sorequired, the Information Officer will provide the data subject with a "POPIA Complaint Form".

12.1.2 Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaintreach the Information Officer within 1 working day.

12.1.3 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

12.1.4 The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.

12.1.5 The Information Officer must also determine whether the complaint relates to anerror or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.

12.1.6 Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will beinformed of this breach.

12.1.7 The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing bodywithin 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate anyanticipated deviation from the specified timelines.

12.1.8 The Information Officer's response to the data subject may comprise any of thefollowing:
12.1.8.1 A suggested remedy for the complaint,
12.1.8.1 A dismissal of the complaint and the reasons as to why it wasdismissed,
12.1.8.3 An apology (if applicable) and any disciplinary action that has beentaken against any employees involved.

12.1.9 Where the data subject is not satisfied with the Information Officer's suggestedremedies, the data subject has the right to complain to the Information Regulator.

12.1.10 The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedurewhere it is found wanting. The reason for any complaints will also be reviewed toensure the avoidance of occurrences giving rise to POPIA related complaints.

## 13 DISCIPLINARY ACTION

13.1 Where a POPIA complaint or a POPIA infringement investigation has been finalised, CTSE may recommend any appropriate administrative, legal and/or disciplinary action tobe taken against any employee reasonably suspected of being implicated in any non- compliant activity outlined within this policy.

13.2 In the case of ignorance or minor negligence, CTSE will undertake to provide furtherawareness training to the employee.

13.3 Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which CTSE may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence tosupport an employee's gross negligence.

13.4 Examples of immediate actions that may be taken subsequent to an investigation include:

13.4.1 A recommendation to commence with disciplinary action to the CEO;

13.4.2 A referral to appropriate law enforcement agencies for criminal investigation.

13.4.3 Recovery of funds and assets in order to limit any prejudice or damages caused.

## 14 LEGISLATIVE FRAMEWORK

14.1 CTSE manages its legislative framework within its defined regulatory and legislative framework as defined within its Compliance Management Policy.

## 15 COMPLIANCE REFERENCES

15.1 Compliance files, policies and manual are maintained by the compliance function. These include:

15.1.1 Compliance Management Policy

Requests for any compliance information or documentation to be submitted to compliance@ctexchange.co.za

## 16 APPROVAL STRUCTURES

16.1 Approval is required by the Board of Directors and Executive Management.

## 17 CONTACT PERSON

The following persons may be contacted in relation to this policy: Deputy Information Officer
Danie Smit dsmit@ctexchange.co.za

Compliance Officer
Palesa Manana palesa@ctexchange.co.za

## 18 ANNEXURES

## ANNEXURE A: PERSONAL INFORMATION REQUEST FORM.

| **Please submit the completed form to the Information Officer:** | |
|---|---|
| Name | |
| Contact Number | |
| Email Address: | |

Please be aware that we may require you to provide proof of identification prior to processing your request.There may also be a reasonable charge for providing copies of the information requested.

| **A. Particulars of Data Subject** | |
|---|---|
| Name & Surname | |
| Identity Number: | |
| Postal Address: | |
| Contact Number: | |
| Email Address: | |

| **B. Request** |
|---|
| I request the organisation to:<br>(a) Inform me whether it holds any of my personal information.<br>(b) Provide me with a record or description of my personal information.<br>(c) Correct or update my personal information.<br>(d) Destroy or delete a record of my personal information. |

| **C. Instructions** |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |

| **D. Signature Page** |
|---|
| Signature<br><br>Date |

## ANNEXURE B: POPIA COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection o Personal Information Act.

| **Please submit your complaint to the Information Officer:** | |
|---|---|
| Name | |
| Contact Number | |
| Email Address: | |

Where we are unable to resolve your complaint, to your satisfaction you have the right to submit a complaint to the Information Regulator.

**The Information Regulator**:**Physical Address: JD House, 27 Siemens Street, Braamfontein, Johannesburg, 2001**

**Email:**

**Website: https://www.justice.gov.za/inforeg**

| **A. Particulars of Complainant** | |
|---|---|
| Name & Surname | |
| Identity Number: | |
| Postal Address: | |
| Contact Number: | |
| Email Address: | |

| **B. Details of Complaint** |
|---|
| |
| |
| |
| |
| |

| **C. Desired Outcome** |
|---|
| |
| |
| |
| |
| |

| **D. Signature Page** |
|---|
| Signature:<br><br>Date |

## ANNEXURE C: POPIA NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us, and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information please request us to update or correct it.

**Our Information Officer's Contact Details**

Name: Eugene Booysen

Email Address: eugeneb@ctexchange.co.za

Purpose for processing your Information.

We collect and hold personal information directly from you through our authorised users or when you use our portals. Information collected may include, inter alia, information to comply with the FICA requirements such as:

- Name and Surname
- Title
- Age
- Date of Birth
- ID number
- Gender
- Marital status
- Nationality
- Physical and Postal address
- Email address
- Telephone number
- Cellphone number
- Online identifier (e.g. Investor number)
- To comply with any legal and regulatory requirements
- To confirm, verify and update your details.

Consent to Disclose and Share your Information.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I **hereby authorise and consent to the organisation sharing my personal information with the following persons:**

Name & Surname

SignatureDate

## ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- **"Personal Information" (PI)** shall mean the 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 of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the Biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitlyof a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- **"POPIA"** shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.
- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
    - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
    - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee's PIby the employer for the purposes of securing and further facilitating the employee's employment with the employer.
    - Without derogating from the generality of the aforestated, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
    - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
    - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
    - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
    - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
    - The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
    - The employee acknowledges that while the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.
- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee herebyagree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.
- Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.

## ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the 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 of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the Biometric informationof the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the **PI** and that the information may have value.

- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.

- Unless so required by law, the parties agree that it shall not disclose any **PI** as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any **PI** out of the Republic of South Africa.

## ANNEXURE F: INFORMATION OFFICER APPOINTMENT LETTER

I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act(Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

| **I hereby accept the appointment as Information Officer** |
| --- |
| Name & Surname<br><br>Signature<br><br>Date |