ONESPACE GROUP OF COMPANIES

Comprising:

- **OneSpace Technologies (Pty) Ltd;**
- **Gatebook (Pty) Ltd;** and
- **BeSecure (Pty) Ltd.**

(Collectively referred to as "**the Organisation**")

DATA PROTECTION

&

RETENTION POLICY

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The OneSpace group of companies (collectively referred to as "**the Organisation**") comprises:

- **OneSpace Technologies (Pty) Ltd;**
- **The Gatebook (Pty) Ltd;**
- **BeSecure (Pty) Ltd.**

1.2 The Organisation is obliged to comply with POPIA and data protection standards.

1.3 The Organisation provides a range of services to its Customers as well as the management of its own Employees, which requires access to and the processing of Personal Data.

1.4 The Organisation is committed to protecting a Person's privacy and ensuring that their Personal Data is used and recorded appropriately, transparently, securely and in accordance with applicable laws.

1.5 This Policy sets out how the Organisation shall process, handle and store Personal Data to comply with its data protection and privacy standards and as well as legislation.

2. DEFINITIONS AND INTERPRETATION

2.1. Unless otherwise expressly stated, or the context otherwise requires, the words and expressions listed below shall, when used in this Policy bear the meanings ascribed to them below and cognate expressions bear corresponding meanings:

2.1.1. "**ANPR**" means automatic number plate recognition software/devices;

2.1.2. "**Board**" means the board of Directors of the Organisation serving from time to time;

2.1.3. "**Confidential Information**" means confidential information relating to the Organisation, including but not limited to: trade secrets, confidential information (i.e. information that is not known in public), technical know-how and data, drawings, system, methods, software processes, client lists, programs, marketing and/or financial information except where such information must be shared between the Organisation and an Employee or between Employees for the purpose of employment or association with the Organisation. Confidential Information includes Personal Information;

2.1.4. "**Consent**" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;

2.1.5. "**Data Breach Plan**" means the Organisation's Data Breach Incident Management Protocol, as amended from time to time;

2.1.6. "**Data Protection Rules**" means any technological, organisational or operational data protection standard, rule, custom, instruction, policy, practice, and/or protocol, whether verbal or in writing;

2.1.7. "**Data Register**" means a register of all processing activities and systems of the Organisation concerning Personal Data set in a format similar to Annexure "**A**";

2.1.8. "**Data Subject**" means the Person to whom Personal Data relates;

2.1.9. "**Directors**" means those persons appointed as directors to the Board according to the Organisation's memorandum of incorporation;

2.1.10. "**Equipment"** means computers, laptops, mobile phones, servers, cameras, access controls, software, cloud storage and other electronic devices;

2.1.11. "**Employee**" means an employee of the Organisation, whether permanent or temporary;

2.1.12. "**Information Officer**" means the information officer appointed by the Organisation from time to time;

2.1.13. "**Information Regulator**" means the information regulatory body established under section 39 of POPIA contactable at:

Email: inforeg@justice.gov.za / Tel: 012 406 4818 / Fax: 086 500 3351.

2.1.14. "**Level of Risk**" means the magnitude of a risk expressed in terms of the combination of consequences and their likelihood assessed and characterized as low, medium and high;

2.1.15. "**Operator**" means a person who processes Personal Data for or on behalf of a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party;

2.1.16. "**Organisation**" means the OneSpace group of companies comprising:

- OneSpace Technologies (Pty) Ltd (2020/115413/07);
- The Gatebook (Pty) Ltd (2015/337250/07);

- BeSecure (Pty) Ltd (2017/103839/07).

2.1.17. "**PAIA**" means the Promotion of Access to Information Act 2 of 2000, as amended from time to time;

2.1.18. "**Person**" means a natural person or juristic person and may include a customer, Employee, independent contractor, job applicant, and vendor;

2.1.19. "**Personal Data**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-

2.1.19.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

2.1.19.2. information relating to the education or the medical, financial, criminal or employment history of the person;

2.1.19.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.1.19.4. the biometric information of the person;

2.1.19.5. the personal opinions, views or preferences of the person;

2.1.19.6. 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;

2.1.19.7. the views or opinions of another individual about the person; and

2.1.19.8. 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;

2.1.20. "**POPIA**" means the Protection of Personal Information Act 4, 2013, as amended from time to time;

2.1.21. "**Privacy Policy**" means the Organisation's Privacy Policy(ies) as amended from time to time;

2.1.22. "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Data, including—

2.1.27.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.1.27.2. dissemination by means of transmission, distribution or making available in any other form; or

2.1.27.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.1.23. "**Responsible Party**" means the person who determines the essential means and purpose for processing Personal Data, including where such Person outsources part or all of the processing to an Operator;

2.1.24. "**Risk Assessment**" means the process to comprehend the nature of the risk and to determine the 'Level of Risk';

2.1.25. "**Subject Access Request**" means a request by a Person to access or alter his/her Personal Data held by the Organisation, whether in person or by email or telephone;

2.1.26. "**this Policy**" means this Data Protection Policy.

2.2. In this Policy:

2.2.1. table of contents and paragraph headings are for purposes of reference only and shall not be used in interpretation;

2.2.2. unless the context clearly indicates a contrary intention, any word connoting any gender includes the other genders, and the singular includes the plural and vice versa;

2.2.3. When a number of days are prescribed such number shall exclude the first and include the last day unless the last day is not a business day, in which case the last day shall be the next succeeding business day.

3. AIM OF THIS POLICY

3.1. This Policy seeks to ensure that the Organisation:

3.1.1. complies with POPIA for the Processing of Personal Data of Data Subjects, both as received from its clients, and as held in respect of its Employees;

3.1.2. protects the rights of its Employees, clients and third parties concerning their Personal Data; and

3.1.3. transparently explains how it Processes Personal Data.

4. SCOPE AND APPLICATION

4.1. This Policy applies to all Personal Data processed by the Organisation including, Personal Data relating to the Organisation's customers, Employees, shareholders, suppliers and agents, irrespective of whether the Personal Data is stored electronically, digitally, on paper, or on other materials, or through other methods.

4.2. This Policy applies to all Employees of the Organisation.

4.3. Where practical, Operators processing Personal Data on behalf of the Organisation should be held to similar or higher standards set in this Policy.

4.4. This Policy shall be reviewed at least annually by the Information Officer.

5. INFORMATION OFFICER

5.1. The chairperson of the Board shall be the Information Officer, unless he designates and appoints an Information Officer who shall register as the Information Officer under POPIA.

5.2. The Information Officer shall, among others:

5.2.1.1. execute, and bear its responsibilities as prescribed in POPIA, PAIA and their respective regulations;

5.2.1.2. ensure that all operational and technological data protection standards are complied with;

5.2.1.3. attend to requests from individuals to access Personal Data which the Organisation holds about them ("**Subject Access Requests**").

6. RESPONSIBLE PARTIES

6.1. All Employees and Operators shall be responsible for ensuring the safeguarding, protection of Personal Data in the execution of their employment duties or rendering services to or for the Organisation.

6.2. The Information Officer shall take responsibility for the Organisation's ongoing compliance with this Policy.

7. DATA CATEGORISATION

7.1. The Organisation may process the following categories (types) of Personal Data:

7.1.1. **Identity Information –** including names, company names, title, date of birth, gender, race and legal status, copies of identity documents or driver's licenses, photographs, identity numbers, signatures, and registration numbers;

7.1.2. **Children Information,** where an instruction is given or action is taken by the Client (Responsible Party) consent is granted by the Parent or Guardian or an Employee as a legal guardian or where it is required by law for the reporting of criminal activities;

7.1.3. **Contact Information –** including billing addresses, delivery addresses, e-email address and telephone numbers**;**

7.1.4. **Criminal Information**, where permitted, including criminal history and ongoing criminal activity collected from law enforcement databases and customer's assets, which is processed on behalf of customers;

7.1.5. **Financial Information -** including bank account details, insurance information, financial statements and tax numbers;

7.1.6. **Location Information -** including data identifying the actual location of assets owned by customers and operated in conjunction with the Organisation;

7.1.7. **Marketing and Communications Information -** including customer and prospective customer preferences in respect of receiving marketing information from us and their communication preferences;

7.1.8. **Sensitive Information –** limited to information concerning employees' race and health status where required by law, where required;

7.1.9. **Fingerprint Information –** collected, processed and retained on behalf of our customers;

7.1.10. **Technical Information -** including internal internet protocol (IP) addresses, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, on the devices used to access our website or networks;

7.1.11. **Usage Information -** including information as to the access and use of our website, products and services.

7.2. For purposes of this Policy, the importance of Personal Data shall be determined with reference to the:

7.2.1. type of Personal Data;

7.2.2. purpose of the Personal Data;

7.2.3. relationship between the Organisation and the Data Subject;

7.2.4. Level of Risk of unauthorised disclosure or access to the Personal Data;

7.2.5. the likely harm or impact on the data subject arising from unauthorised disclosure;

7.2.6. requirements of the ruling regulatory framework applicable to that Personal Data and relationship.

7.3. Children, Criminal, Financial and Sensitive Information shall always be categorised as highly important and high-risk Data.

8. DATA REGISTER

8.1. To ensure its processing of Personal Data is lawful, fair and transparent, the Organisation shall maintain a Data Register, which shall be reviewed annually.

8.2. The Data Register will provide a record of the Organisation's processing activities together with a list of the Organisation's Operators.

9. REQUESTS FOR ACCESS TO OR ALTERATION OF DATA

9.1. Employees and Persons who are the subject of Personal Data held by the Organisation are entitled to make a Subject Access Request to the Organisation.

9.2. Subject Access Requests should be made by e-mail and addressed to the Information Officer, who shall consider and respond to the request within 30 days of the request.

9.3. The identity of a person making a Data Subject request shall be verified using appropriate and proportionate security questions before handing over any Personal Data requested.

10. LAWFUL PURPOSE

10.1. All Personal Data processed by the Organisation must rely on a legal basis permitted by section of 11 of POPIA.

10.2. The Organisation shall note the appropriate lawful basis for each processing activity in the Data Register.

10.3. Where consent is relied on for Processing, the Organisation shall allow the Data Subject the ongoing opportunity to revoke such consent.

10.4. Where the Organisation relies on a legitimate interest ground, this legitimate interest should be explained in the relevant privacy notice.

11. DATA MINIMISATION

11.1. The Organisation shall process the minimum Personal Data needed to perform its Processing activities to achieve the purpose of such activities.

11.2. The Organisation shall take reasonable steps to prevent it Processing unnecessary Personal Data for that specific Processing activity. The Organisation will minimise unnecessary Data collected by, among others, using privacy by design measures and technology.

11.3. Should the Organisation obtain Personal Data not requested or unnecessary for the performance of an activity, such Personal Data shall be destroyed or anonymised.

11.4. The Organisation shall ensure that, when verifying the identify of Persons in handling any requests, the verification method must be proportionate to the initial verification method used to collect the Personal Data.

12. DATA ACCURACY AND INTEGRITY

General

12.1. The Organisation and its Employees shall take all reasonable steps to comply with the Organisation's Data Protection Rules to ensure Personal Information is kept accurate and up to date.

12.2. The Organisation shall require contracted parties to notify the Organisation when their information is inaccurate or out of date.

12.3. If Personal Data is of a higher level of importance, greater and more frequent efforts shall be implemented to maintain its accuracy.

12.4. The Organisation shall take appropriate measures to prevent accidental or unauthorised deletion of records containing Personal Data.

12.5. Backup procedures shall be implemented on servers to ensure data integrity and protect against data loss from drive failure.

Customer Data

12.6. Generally, the accuracy of customer Personal Data shall be regularly reviewed by the Organisation through direct communications with the Data Subject.

Data collected from third parties

12.7. Where the Organisation becomes aware of inaccurate or misleading Data supplied by third parties, the Organisation will take reasonable steps to mitigate or eliminate any risk of harm resulting from its processing of such Data.

12.8. If the Organisation becomes aware of any database provider holding inaccurate records, the Organisation may notify and choose to suspend collection of Data from such database provider.

13. ARCHIVING AND RETENTION

13.1. The Information Officer is responsible for the continuing process of identifying the records that have met their required retention period.

13.2. The Organisation shall maintain record management rules and procedures to identify, monitor and destroy unnecessary records after they are no longer required.

13.3. Personal Data shall not be retained for longer than necessary, but this will be dependent on the importance of the Personal Data.

13.4. The general data retention period shall be for a period of 5 (five) years after the relevant contract or transaction comes to an end, whereafter such files shall be destroyed in accordance with this Policy.

13.5. **Annexure** "**B**" sets out the general statutory retention periods. Other data retention periods are set out below:

13.5.1. **Records held in terms of the Companies Act, 2008** - the Organisation shall retain accounting records as well as records related to shareholders and directors for a period of 7 (seven) years, or so long as may be prescribed by law (from time to time).

13.5.2. **Customer Data** – the Organisation shall retain, for a period of 5 (five) years from the date of last entry or document on file, all accounting records, files, transactions, and documents relating to matters dealt with by the Organisation on behalf of customers. Where legislation prescribes longer periods for specific customer Data, such longer periods shall apply.

13.5.3. **Customer contact Data** – contact information may be retained while they are a customer, after which the Data Subject usually becomes a prospective customer;

13.5.4. **Prospective customer contacts** – contact information retained for 2 (two) years after the date of last entry or document on file, or until it is identified that the prospective customer no longer has an interest in the services;

13.5.5. **Employees** – written particulars of Employees, including identifiable information, period of employment, remuneration paid, employee loans and any other prescribed information is to be retained while employed and for a period of 5 (five) years after termination of employment or so long as may be prescribed by law;

13.5.6. **Contractors** – any Personal Data required for the purposes of the service delivery will be retained for a period of 3 (three) years after termination of the contract or longer where legal obligations require it (i.e FICA).

13.5.7. **Potential Employees** - CVs and covering letters enclosing Personal Data will be retained for 8 (eight) months in a centralised folder after an application has completed, or longer where legal obligations or litigation necessitate it.

13.5.8. **ANPR and related Data (Gatebook & SNIPR)** – vehicle number plate Data and incident reports are retained, in a pseudonymised format, for a period of up to 5 years (unless instructed otherwise) from collection pursuant to the legitimate interests of the Organisation, our customers, our customer's customers, and the general public in detecting and preventing imminent threats to life and property.

13.5.9. **CCTV (SNIPR)** – we retain any CCTV footage for 6 weeks or as long as necessary to comply with any investigations by law enforcement, however our customers may select their own retention periods for their assets.

13.5.10. **Visitor Data (Gatebook)** – customers are able to configure their retention periods on our system(s), however by default to limit possible harm, we limit the maximum retention period to 3 years.

13.6. Documents that are required to be kept for certain periods of time under the ruling regulatory framework shall be stored in a manner and place that is secure, and if possible, fire resistant.

14. DESTRUCTION OF PERSONAL DATA

14.1. The Information Officer is responsible for the continuing process of supervising the destruction of records containing Personal Data.

14.2. Upon expiry of the retention periods, any Personal Data and/or written or electronic file containing Personal Data that is not being retained or used must be destroyed in a secure manner.

14.3. The Organisation shall use secure methods to destroy Personal Data or records containing Personal Data.

14.4. All unwanted paper records containing any Personal Data must be shredded before being recycled or otherwise disposed of.

15. ASSESSMENTS

15.1. The Organisation may take appropriate measures and assessments to ascertain any new and existing risks concerning its processing, and whether additional or improved technological and organisation measures should be adopted to mitigate or eliminate such risks in a proportionate manner.

16. DATA PROTECTION RULES (SECURITY)

16.1. **Data protection rules are confidential to the Organisation and may only be disclosed with the prior written approval of the Information Officer as its disclosure may impair or undermine the aim of this Policy.**

16.2. Data protection rules are also risk-based and may be adjusted or changed at any time whether verbally or otherwise to ensure adaptive, responsive, efficient and functional data management to address evolving organisational and technical risks. **On this basis, not all data protection rules may be captured in writing**.

16.3. The Organisation ensures that appropriate and necessary data protection measures are taken to protect Personal Data.

16.4. The Organisation sets out common examples of some of the measures taken to protect Personal Data.

16.4.1. TECHNICAL SECURITY MEASURES

Common examples

(1) Electronically stored Personal Data will be protected from unauthorised access and accidental deletion by using passwords, encryption, file permission controls, and other similar measures.

(2) Wherever feasible, Personal Data shall be encrypted before being transmitted and stored electronically at a level suitable to its risk.

(3) All servers containing Personal Data shall be in secure protected data servers with appropriate security measures, such as physical and electronic access controls, and redundant generators/power supply and distribution.

(4) The Organisation may use hosted servers located within the Republic of South Africa, or any other territory with adequate data protection laws in terms of POPIA.

16.4.2. ORGANISATIONAL SECURITY MEASURES

Common examples

(1) The Organisation follows a Data Breach and Incident Management Plan.

(2) All Personal Data is deemed Confidential Information, and will be handled with a higher degree of care and skill than ordinary information.

(3) Employees shall sign confidentiality undertakings (alternatively their employment contracts must provide for similar obligations).

(4) The only Employee/s entitled to access Personal Data, will be those who need to access it for the execution of their direct work or required outputs.

(5) Employees will receive induction and on-the-job training in relation to all security standards applicable to operations.

(6) Employees shall keep all Personal Data secure by taking sensible practical precautions and complying with all data protection rules.

(7) Employees and Operators are entitled to access only those elements of IT and paper filing systems that are consistent with their authorization and purpose for processing the Personal Data.

17. DISCLOSURE WITHOUT CONSENT

17.1. The Organisation may be authorised by law, in limited circumstances, to disclose or provide Personal Data to regulatory authorities, other agencies or security providers in circumstances where the Consent of the Data Subject has not been obtained or required.

17.2. In the above circumstances, the Organisation may be obliged to disclose the requested Personal Data, but will first ensure that the request is legitimate.

18. DATA BREACHES

18.1. Any Employee, Operator, supplier, or service provider shall immediately notify the Information Officer of any suspected or actual data breach or compromise of Personal or Confidential Information as soon as they become aware of or ought reasonably to have become aware of such suspected or actual breach.

18.2. The Information Officer is responsible for managing Personal Data and other Confidential data security breaches in conjunction with the Privacy Committee.

19. EMPLOYEES' CODE OF CONDUCT

19.1. This Policy sets out workplace rules governing Employees in the course of their work and services to the Organisation. It shall form part of and is hereby incorporated into the Organisation's disciplinary codes and procedure.

19.2. A breach of any rule in relation to the protection of Personal Data set out in this Policy shall form the basis of disciplinary action and, in appropriate circumstances, may lead to dismissal.

19.3. Every Employee must familiarise him/herself with the contents of this Policy, and must remain up to date as and when it is notified of any changes to this Policy in writing (including email correspondence and/or website notification).

20. RESPONSIBLE PARTY FOR PERSONAL AND OTHER CONFIDENTIAL DATA BREACHES

21. POLICY ADMINISTRATION

Information Officer Details

Name : Mrs. Jess Roux
E-mail Address : jess@one-space.co.za
Telephone Number during office hours (08H00 – 17H00) (Tel: (031) 035 0941)
After Hours phone will be answered by on-call staff and redirected as required.

22. REVISION HISTORY

Version Number	Purpose of revision	Review date	Effective date	Summary of key points
V2	New Policy	30 June 2021		Establishment of Policy

ANNEXURE B

STATUTORY RETENTION PERIODS

Legislation	Document	Retention Period
Companies Act 71 of 2008	Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; Copies of reports presented at the annual general meeting of the company; Copies of annual financial statements required by the Act; Copies of accounting records as required by the Act; Record of directors and past directors, after the director has retired from the company; Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee and directors' committees.	7 years
	Registration certificate; Memorandum of Incorporation and alterations and amendments; Rules; Securities register and uncertified securities register; Register of company secretary and auditors and Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply); Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	Indefinitely
Consumer Protection Act of 2008	Full names, physical address, postal address and contact details; ID number and registration number;	3 years

	Contact details of public officer in case of a juristic person; Service rendered; Cost to be recovered from the consumer; Frequency of accounting to the consumer; Amounts, sums, values, charges, fees, remuneration specified in monetary terms; Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions	
Financial Intelligence Centre Act	Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; The manner in which the identity of the persons referred to above was established; The nature of that business relationship or transaction; In the case of a transaction, the amount involved and the parties to that transaction; All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; Any document or copy of a document obtained by the accountable institution	5 years
Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
	Section 20(2) documents : -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;	3 years

	-Records of incidents reported at work.	
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; **Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):** -Records of risk assessments and air monitoring; -Medical surveillance records. **Lead Regulations, 2001, Regulation 10**: -Records of assessments and air monitoring; -Medical surveillance records N**oise records - induced Hearing Loss Regulations, 2003, Regulation 11**: -All records of assessment and noise monitoring; -All medical surveillance records, including the baseline audiogram of every employee.	40 years
	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; -Medical surveillance records	30 years
Basic Conditions of Employment Act	**Section 29(4):** -Written particulars of an employee after termination of employment; **Section 31**: -Employee's name and occupation; -Time worked by each employee;	3 years

	-Remuneration paid to each employee; -Date of birth of any employee under the age of 18 years	
Employment Equity Act	Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General	
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	
	An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite
UIF Act	Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed	5 years
Tax Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -Will enable SARS to be satisfied that the person has observed these requirements	5 years

Income Tax Act	Amount of remuneration paid or due by him to the employee; The amount of employees tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information; Employer Reconciliation return	
Value-Added Tax Act	Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; Documentary proof substantiating the zero rating of supplies; Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	