DATA RETENTION, ARCHIVING AND DESTRUCTION POLICY

1. INTRODUCTION

1.1 This Data Retention, Archiving and Destruction Policy (the "Policy") has been created in order to set out the principles for retaining and destroying specified categories of data. This policy specifies how important documents (hardcopy, online or other media) should be retained, protected and eligible for destruction.

1.2 This Policy should be read in conjunction with other policies that have as their objectives the protection and security of data.

1.3 This Policy applies to all Company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to Data. It is the responsibility of all the above to familiarise themselves with this Policy and ensure adequate compliance with it.

1.4 This Policy covers all data processed within the company.

1.5 Tis policy applies to the principles of data and information security in line with relevant legislation and the Company's business strategies and objectives.

1.6 This policy applies to the relationship of the Company with its personnel, clients and associates and is based on mutual integrity and trust and it is therefore committed to maintaining this trust by protecting the privacy of personal information and data disclosed and received from any data subject or data owner at all times and to the best of its ability.

2. DEFINITIONS

2.1. "Account Data" consists of cardholder data and/or sensitive authentication data.

2.2. "Anonymisation" is the process of turning data into a form which does not identify individuals. It is a type of information sanitization whose intent is privacy protection.

2.3. "Archiving" is the process of moving data that is no longer actively used to a separate storage device or location for retention.

2.4. "Asset Owner" is the Functional or Business Line Head who is responsible for the Data. Asset (or within whose function or business line the Data Asset resides or is used).

2.5 "Data" is Record and Document.

2.6 "Data Asset" is any item or entity that comprises data. For example, databases are data asset that comprise records. A data asset may be a system or application output file,

database, document, or webpage. A data asset may also include a means to access data from an application.

2.7 "Data Processing" is the collection and manipulation of data to produce meaningful information. Processing includes transformation, accessing, updating, transferring, destruction and any other manipulation of data.

2.8 "Destruction" is defined as physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially available means.

2.9 "Document" as used in this Policy, is any medium which holds Information used to support an effective and efficient organizational operation.

2.10 "Personal Data" (also "Personally Identifiable Information") is any information relating to an identified or identifiable natural person (the "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.11 "Record" as used in this Policy, is any medium which holds information or evidence about a past event. Examples of Records include: Meeting records, Reports, Minutes, Video and audio recordings

2.12 "Data Processing" The collection, transformation, accessing, updating, transferring, destruction and any other manipulation of data.

2.13 "Retention" is the continued processing of data, after the initial "Active Use" has achieved the purpose for which the data was originally collected. Data Retention is usually required to meet applicable legal or contractual obligations or meet business objectives. Retention Periods are determined accordingly. For Personal Data they must be no longer than necessary to protect the rights and freedoms of individual data subjects in accordance with International SOS Data Protection Policy and applicable Data Protection regulation.

3. PURPOSE OF THE POLICY

The purpose of this Policy is to enable the Company to:

a) Comply with relevant legislation in respect of Personal Information it processes / retains about Personnel / Staff, directors, Visitors, Members and contractors / service providers; and

b) To follow good practice and to protect Personnel / Staff, directors, Visitors and Members; and

c) To respect individual's rights; and

d) To ensure that any Personal Information held is not being misused; and

e) To protect the Company from the consequences of a breach of its responsibilities

4. GENERAL PRINCIPLES OF DATA RETENTION

4.1 The Company is bound by various obligations with regard to the data that we process or control. These obligations include how long we may retain Data and when and how we can destroy it. The obligations may arise from industry standards, legislation or regulations or from contracts and agreements parties.

4.2 The Company may further be involved in unpredicted events such as litigation or business disaster recoveries that require us to have access to the original Data in order to protect the interests of the Company or those of our employees, customers, goods and service providers and our partners.

4.3 As a result, Data may need to be archived beyond its active use. A contract may, for example, expire after two years but other Data may, by law, need to be retained for a longer period.

4.4 When the Document Retention Period for a particular type of data is over, the Company is required to destroy that data in a secure manner, unless a documented exception is agreed on.

4.5 To effectively protect data subjects' right to privacy and comply with regulatory requirements, it is important to apply certain principles when processing Personal Data. This will determine retention periods for data that falls into this category.

4.6 Personal Data should only be retained as long as is necessary for each specific purpose for which it was collected.

4.7 Personal Data should be kept up-to-date and accurate. Ensuring that records containing Personal Data are disposed of when no longer needed will reduce the risk that such data will become inaccurate, out of date or irrelevant and that it may be used in error.

4.8 Accurate and up-to-date records of Personal Data Processing Activities must be maintained.

5. DATA INVENTORIES

5.1 Documents and Records should be organised into Data Assets such as SharePoint sites, databases or electronic information systems (examples would be a payroll system) to allow systematic, standardised management.

5.2 Data Management outside of such systems must be reduced to a minimum.

5.3 It is the responsibility of the respective Departmental Manager to ensure that each of the Company Data Assets are registered on the Inventory by the nominated Asset Owner.

5.4 Each Data Asset is subject to a specific retention period for the data, reflecting the legitimate basis justifying the need for and use of the Data. Retention periods for different types of Data will depend on the nature of such Data.

5.5 Asset Owners are to ensure that their Data Asset Inventory entries are reviewed, and if necessary updated, at least annually and every time significant changes are made to a process involving a Data Asset assigned to them.

5.6 It is the responsibility of the respective Departmental Managers to ensure that all Personal Data Processing are recorded on the Data Processing Inventory.

5.7 For each Processing Activity, the following should be recorded:

i. Purpose of Processing

ii. Data Subject Type

iii. Data Type

iv. Location / Data Asset

v. Lawful basis of Processing

vi. Whether the data contains Sensitive Personal Data

vii. Start of Retention, Retention Periods and Archival (if applicable)

5.8 The respective Departmental Managers are to ensure that their Inventory entries are reviewed, and if necessary updated, at least annually and every time significant changes are made to a process.

6. DATA RETENTION AND ARCHIVING

All Personnel are responsible for ensuring that any Personal Information which they hold is kept securely and that they are not disclosed to any unauthorized third party.

6.1 Retention and Archiving Period

6.1.1 For the purposes of enforcing Retention in accordance with this Policy, each function is responsible for the Records and Documents it creates, uses, stores, processes and destroys. These lists of Record and Document types shall be

maintained by each Function under guidance from the Compliance Department.

6.1.2` All staff are required to establish the record retention periods under the advice of the Company. These retention periods should be submitted during the annual compliance audits.

6.1.3 Retention periods shall not be exceeded without prior written authorisation.

6.2 **Safeguarding of Information in terms of Archiving**

6.2.1 All archived data must be encrypted or locked and continuously safeguarded to avoid data breaches.

6.2.2 Paper Records shall be archived in secured storage onsite or secured offsite location, clearly labelled in archive boxes naming the date upon which such information is to be destroyed.

6.2.3 Electronic Records shall be archived in accordance with the Information Security Standards for access controls and in a format which is appropriate to secure the confidentiality, integrity and accessibility of the Documents. After the archival period has expired records shall be destroyed.

6.2.4 An archiving period more or less than the period as determined by the Company may be granted by exception. The employee will request an exception to be submitted to the Information Officer to archive such Records. Such exception request shall specify the administrative, organizational and technical measures to be undertaken to ensure the confidentiality, integrity and availability of such Records.

6.2.5 All backups of information are stored securely in the cloud.

6.2.6 Employees may not copy software illegally. Under South African Copyright Law, an employee who uses illegal copies of software can expose The Company to substantial fines and possible claims for damages. It is a criminal offence to copy or use pirated software. Accordingly, The Employee may be criminally prosecuted, which could lead to heavy fines or possible imprisonment. Permission from the IT-Supervisor or Service Provider is required before loading any non-Company software onto a Company machine;

6.2.7 All software used for and on behalf of The Company shall be correctly and appropriately licensed and used only in conformity with the terms of the license.

6.2.8 Any employee found to be using illegal software on a company device will be subject to disciplinary measure.

7. DESTRUCTION OF DATA

7.1 All Data, whether held electronically, on individual employees' devices or on paper, should be reviewed on a regular basis to decide whether to destroy or delete any Data in accordance with the designated retention period.

7.2 Responsibility for the destruction of data included in the Data Asset Inventory falls to each Asset Manager.

7.3 Responsibility for the destruction of data included in local departmental document and record inventories falls to each Departmental Manager.

7.4 Personal Data or confidential or restricted information must be disposed of as confidential waste and be subject to secure electronic deletion or Anonymisation.

7.5 Paper Documents shall be shredded using secure, locked consoles designated.

7.6 The Company shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files.

7.7 When the company receives an email query such query will be attended to within reasonable time. Once the query has been sufficiently responded to the company will retain such email for a period of two week and then such email may be deleted from the company server.

7.8 The Company shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

7.9 The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Company subcontracts for this purpose. All external service providers must be thoroughly vetted and reviewed to ensure their full compliance with data protection requirements.

7. RESPONSIBILITIES

7.1 Information Officer

7.1.1 The Information Officer may audit compliance with this Policy from time to time and provide recommendations to be reviewed by the relevant senior management.

7.1.2 The Information Officer shall provide guidance with regard to this Policy.

7.1.3 Ensure compliance with the Policy and POPIA.

7.1.4 Ensure that all Personal Information processed is always secured and kept confidential, save as where disclosure is required in terms of the Law.

7.1.5 Ensure all contracts contain a clause regarding POPIA compliance.

7.1.6 Ensure that all Personal Information is accurate, complete, and up to date

7.1.7 Ensure all Personal Information is kept safely and securely.

7.1.8 Always ensuring adequate safeguards in place.

7.1.9 Provide access to Personal Information when required to do so in terms of applicable legislation

7.1.10 Ensure Personal Information is destroyed when required.

7.1.11 Assist the Information Regulator in respect of any investig

7.1.12 Handling all aspects of relationship with the Regulator

7.1.13 Notify persons as well as Regulator immediately in the event of a breach

7.1.3 The Information Officer shall administrate and oversee the use of Data Asset and Personal Data Processing Inventory systems.

8.2 All Employees

8.2.1 Employees are responsible for the data the they creates use, store, process and destroy.

8.2.2 Each employee must familiarise themselves with the policies relating to the retention, archiving and destruction of data

8.2.3 Each employee shall be responsible for returning Records and Documents in their possession or control to the Company upon separation or retirement.

8.2.4 Final disposition of such Records and Documents shall be determined by the Company in accordance with this policy and the respective country employee exit process.

9. ENFORCEMENT AND REPORTING BREACHES

9.1 Breaches of this Policy may have serious legal and reputation repercussions and could cause material damage to the Company. Consequently, breaches can potentially lead to disciplinary action that could include summary dismissal and to legal sanctions, including criminal penalties.

9.2 All employees are expected to promptly and fully report any breaches of the Policy. A report may be made to the employees' supervisor or the Information Officer.

9.3 The report must contain at the minimum the following:

- A description of the possible consequences of the security compromise;
- A description of the measures taken or proposed to be taken by the responsible party to remedy the security breach;
- A recommendation of the measures that any party whose personal information was leaked in the security compromise should take in order to mitigate the possible adverse effects of the security compromise;
- The identity of the unauthorised person, if known, who accessed or acquired the personal

9.4 A deliberate failure by an employee or staff member to report a breach will lead to disciplinary measure to be instituted by the company.