SENTRAAL-SUID KOÖPERASIE Bpk.
SENTRAAL-SUID CO-OPERATIVE Ltd.

POLICY STATEMENT AND MANUAL OF:

PROTECTION OF PERSONAL INFORMATION AND THE

RETENTION OF DOCUMENTS

FOR

SENTRAAL-SUID Co-operative Ltd.

(hereinafter referred to as "SSK")

(Registration number: 1943/000002/24)

Index

A. SSK POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

1. PURPOSE

1.1 To exercise effective control over the retention of documents and electronic transactions:

1.1.1 as prescribed by legislation;

and 1.1.2 as dictated by business practice.

1.2 Documents need to be retained in order to prove the existence of facts and to exercise rights the Co-operative may have. Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of the Co-operative and to minimize the Co-operative's reputational risks.

1.3 To ensure that the Co-operative's interests are protected and that the Co-operative's and business partners' rights to privacy and confidentiality are not breached.

1.4 Queries may be referred to the SSK Information Officer or the Co-operative Secretary. (Refer to Section B 6 below for contact details)

2. SCOPE AND DEFINITIONS

2.1 All documents and electronic transactions generated within and/or received by the Co-operative.

2.2 Definitions:

2.2.1 **Business partners** includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Co-operative.

2.2.2 **Confidential Information** refers to all information or data disclosed to or obtained by the Co-operative by any means whatsoever and shall include, but not be limited to:

2.2.1 financial information and records; and

2.2.2 all other information including information relating to the structure, operations, processes, intentions, product information, know-how, trade secrets, market opportunities, customers and business affairs but excluding the exceptions listed in clause 4.1 hereunder.

2.2.3 **Constitution:** Constitution of the Republic of South Africa Act, 108 of 1996.

2.2.4 **Data** refers to electronic representations of information in any form.

2.2.5 **Documents** include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

2.2.6 **ECTA:** Electronic Communications and Transactions Act, 25 of 2002.

2.2.7 **Electronic communication** refers to a communication by means of data messages.

2.2.8 **Electronic signature** refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

2.2.9 **Electronic transactions** include e-mails sent and received.

2.2.10 **PAIA:** Promotion of Access to Information Act, 2 of 2000.

3. ACCESS TO DOCUMENTS

3.1 All Co-operative and business partner information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 4.2 below):

3.1.1 where disclosure is under compulsion of law;

3.1.2 where there is a duty to the public to disclose;

3.1.3 where the interests of the Co-operative require disclosure; and

3.1.4 where disclosure is made with the express or implied consent of the business partner.

3.2 Disclosure to 3rd parties:

All employees have a duty of confidentiality in relation to the Co-operative and business partners. In addition to the provisions of clause 3.1 above, the following are also applicable:

3.2.1 Information on business partners: Our business partners' right to

confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the business partner has consented in writing to that person receiving the information.

3.2.2 Requests for Co-operative information:

3.2.2.1 These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Co-operative, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

3.2.2.2 In terms hereof, requests must be made in writing on the prescribed form to the SSK Information Officer, Co-operative Secretary or the Deputy Information Officers. (Refer to Section B 6 below for contact details) The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

3.2.2.3 SSK have a PAIA policy in place. [Refer to the **SSK PAIA policy** and **Annexure 1 – PAIA Request for access to records form** and **Annexure 2 – PAIA fees for request of records form** included in the SSK PAIA policy]

3.2.3 Confidential Co-operative and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Co-operative must be kept strictly confidential at all times.

3.3 The Co-operative views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

4. STORAGE OF DOCUMENTS

4.1 HARD COPIES

Hardcopies of documents are stored in archives at dedicated locations. All hardcopies of documents are retained in line with the guidelines as set out by the SAICA guide on the retention of records document. (Refer to **Annexure 1 – SAICA Retention of Records guide** below for a detailed list of all retention period guidelines for specific types of documents and applicable Acts that these documents apply to.)

4.2 ELECTRONIC STORAGE

4.2.1 The internal procedure requires that electronic storage of information:

important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

4.2.2 Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel.

Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

4.2.3 Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information, and the purpose for which the data was collected, must be kept by the person who electronically requests, collects, collates, processes or stores the information. A record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

5 DESTRUCTION OF DOCUMENTS

5.1 The Information Officer will on a yearly (Preferably in May / June) basis request all Department Heads to identify documents / information that has reached their retention period.

5.2 Each department is responsible for attending to the destruction of its documents. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Co-operative pending such return.

5.3 After completion of the process in 5.2 above, the Department Head shall, in writing, authorise the removal and destruction of the documents. These authorisation requests will be forwarded to the Information Officer for filling / record keeping.

5.4 The documents are then made available for collection by the removers of the Co-operative's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information. Documents may also be stored off-site, in storage facilities approved by the Co-operative.

B. SSK POPI POLICY (IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013)

1. INTRODUCTION

SSK is a group of companies functioning within the agricultural, retail, insurance, finance, grain storage and production space that is obligated to comply with The Protection of Personal Information Act 4 of 2013.

POPIA requires SSK to inform their business partners (Including employees) as to the manner in which their personal information is used, disclosed and destroyed.

SSK guarantees its commitment to protecting its business partner's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The Policy sets out the manner in which SSK deals with their business partner's personal information as well as and stipulates the purpose for which said information is used. The Policy is made available on SSK's website www.ssk.co.za, and on request from SSK head office.

The Policy is drafted in conjunction with the Financial Intermediary Association's ("FIA") Protection of Personal Information Notice.

2. PERSONAL INFORMATION COLLECTED

Section 9 of POPI states that "*Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.*"

SSK collects and processes business partner's personal information pertaining to the business partner's financial needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, SSK will inform the business partner as to the information required and the information deemed optional. Examples of personal information we collect include, but is not limited to: •The Business Partner's Identity number, name, surname, address, postal code, marital

status, and number of dependents;

- Description of the business partner's residence, business, assets; financial information, banking details, etc.; and
- Any other information required by SSK and suppliers in order to provide business partners with an accurate analysis of their business needs.

SSK may also collect and process business partner's personal information for marketing purposes in order to ensure that our products and services remain relevant to our business partners and potential business partners.

SSK aims to have agreements in place with all product suppliers, insurers and third party service providers to ensure a mutual understanding with regard to the protection of the business partner's personal information. SSK suppliers will be subject to the same regulations as applicable to SSK.

With the business partner's consent, SSK may also supplement the information provided with information SSK receives from other providers in order to offer a more consistent and personalized experience in the business partner's interaction with SSK. For purposes of this Policy, business partners include potential and existing business partners.

3. THE USAGE OF PERSONAL INFORMATION

The Business Partner's Personal Information will only be used for the purpose for which it was collected and as agreed.

This may include:

- Providing products or services to business partners and to carry out the transactions requested;
- For underwriting purposes;
- Assessing and processing claims;
- Conducting credit reference searches or- verification;
- Confirming, verifying and updating business partner details;
- For purposes of claims history;
- For the detection and prevention of fraud, crime, money laundering or other malpractices;
- Conducting market or customer satisfaction research;
- For audit and record keeping purposes;
- In connection with legal proceedings;
- Providing SSK services to business partners, to render the services requested and to maintain and constantly improve the relationship;
- Providing communication in respect of SSK and regulatory matters that may affect business partners; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

According to section 10 of POPI, personal information may only be processed if certain

conditions, listed below, are met along with supporting information for SSK processing of Personal Information:

- The business partner's consents to the processing: - consent is obtained from business partners during the introductory, appointment and needs analysis stage of the relationship;
- The necessity of processing: in order to conduct an accurate analysis of the business partner's needs for purposes of amongst other credit limits, insurance requirements, etcetera.
- Processing complies with an obligation imposed by law on SSK;
- The Financial Advisory and Intermediary Services Act ('FAIS') requires Financial Service Provider's ('FSPs') to conduct a needs analysis and obtain information from business partners about their needs in order to provide them with applicable and beneficial products;
- Processing protects a legitimate interest of the business partner — it is in the business partner's best interest to have a full and proper needs analysis performed in order to provide them with an applicable and beneficial product or service; and
- Processing is necessary for pursuing the legitimate interests of SSK or of a third party to whom information are supplied. In order to provide SSK business partners with products and or services both SSK and any of our product suppliers require certain personal information from the business partners in order to make an expert decision on the unique and specific product and or service required.

4. DISCLOSURE OF PERSONAL INFORMATION

SSK may disclose a business partner's personal information to any of SSK companies or subsidiaries, joint venture companies and or approved product- or third party service providers whose services or products business partners elect to use. SSK has agreements in place to ensure compliance with confidentiality and privacy conditions.

SSK may also share business partner personal information with, and obtain information about business partners from third parties for the reasons already discussed above.

SSK may also disclose a business partner's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect SSK rights.

5. SAFEGUARDING BUSINESS PARTNER INFORMATION

It is a requirement of POPI to adequately protect personal information. SSK will continuously review its security controls and processes to ensure that personal information is secure.

The following procedures are in place in order to protect personal information:

5.1 SSK **INFORMATION OFFICER** is Francois Swanepoel whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. He is assisted by Francois Smit who functions as the Deputy Information Officer and acts as Chairman of the POPIA project team;

5.2 A **POPIA PROJECT TEAM** has been established to oversee the implementation, out roll and day-to-day adherence of the policy and POPI Act.

5.3 **THIS POLICY** has been put in place throughout SSK and initial training on this policy and the POPI Act was conducted by SSK training third party service providers and the Group Compliance function. Ongoing training sessions and awareness notifications on the policy and POPI Act the will be provided;

5.4 Each new employee will be required to sign an **EMPLOYMENT CONTRACT** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

5.5 Every employee currently employed within SSK will be required to sign an addendum to their **EMPLOYMENT CONTRACTS** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

5.6 SSK archived business partner information is stored on site which is also governed by POPI, access is limited to these areas to authorized personal.

5.7 SSK product suppliers, insurers and other third party service providers will be required to sign an **AGREEMENT** guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

5.8 All electronic files or data are **BACKED UP** by the IT and Information functions which is also responsible for system security that protects third party access and physical threats. The Group IT Division is responsible for Electronic Information Security;

6. ACCESS AND CORRECTION OF PERSONAL INFORMATION

Business partners have the right to access the personal information SSK holds about them. Business partners also have the right to ask SSK to update, correct or delete their personal information on reasonable grounds.

Once a business partner objects to the processing of their personal information, SSK may no longer process said personal information. SSK will take all reasonable steps to confirm its business partners' identity before providing details of their personal information or making changes to their personal information.

The details of SSK's Information Officer, Deputy Information Officer, Co-operative Secretary and Head Office are as follows:

SSK Information Officer:

Name: Francois Swanepoel
Telephone number: (028) 514 8611
Fax number: (028) 514 8656
E-mail address: francois.swanepoel@ssk.co.za

SSK Deputy Information Officer:

Name: Francois Smit
Telephone number: (028) 514 8665
Fax number: (028) 514 8656
E-mail address: francois.smit@ssk.co.za

SSK Deputy Information Officer:

Name: Alwyn Burger
Telephone number: (028) 514 8628
Fax number: (028) 514 8656
E-mail address: alwyn.burger@ssk.co.za

SSK Deputy Information Officer and Co-operative Secretary:

Name: Villiers van Veen
Telephone number: (028) 514 8607
Fax number: (028) 514 8656
E-mail address: villiers.vanveen@ssk.co.za

Head Office details:

Telephone number: (028) 514 8600
Fax number: (028) 514 8656
Postal address: PO Box 12, Swellendam, 6740
Physical address: 34 Voortrek Street, Swellendam, 6740
E-mail address: info@ssk.co.za
Website: www.ssk.co.za