SUNGROW SOUTHERN AFRICA (PTY) LTD

Protection of Personal Information Act 4 of 2013

DATA PROTECTION POLICY

RECORD

Version	Date	Submitted to	Status
1		BOARD OF DIRECTORS	APPROVED (***INSERT DATE***)

Table of Contents

1. INTRODUCTION

1.1. To meet the key functions, the Company recognises that it must process the Personal Information of its employees, potential consumers, consumers and third parties. In doing so, the Company is committed to the observance of, and compliance with, the directives of the Constitution and national legislation alike, including the Protection of Personal Information Act. The Company endorses the key principles of good governance, transparency and accountability and seeks to regulate the use and Processing of Personal Information as lawfully required.

1.2. The right to privacy forms the cornerstone of information and data protection laws worldwide. Similarly, the Protection of Personal Information Act 4 of 2013, as amended from time to time ("**POPIA**") aims to protect the constitutional right to privacy in South Africa. Information and data protection have become a global issue and stringent protection thereof is now the international norm.

1.3. The "**Company**" (as defined in paragraph 2) qualifies as a Responsible Party contemplated in Chapter 1 of the Act and therefore implements this internal POPIA Policy (as defined in paragraph 2) to establish clear procedures for the Company to comply with the provisions of the Act. This document represents the formulation and implementation of a data protection policy, depicting the internal procedures and policy of the Company as required in terms of POPIA.

2. DEFINITIONS

2.1. "**Company**" means Sungrow Southern Africa (Pty) Ltd, a company registered in accordance with the laws of South Africa under registration number 2017/217975/07;

2.2. "**Compliance Framework**" the framework established in terms of this Policy of the Company and detailed in paragraph 4, and which is aimed at promoting and ensuring compliance by the Company with its obligations in terms of the Act;

2.3. "**Data Subject**" a person to whom Personal Information relates and is therefore the party whose Personal Information is Processed by Responsible Parties. Data Subjects include identifiable, living natural persons and if applicable, an identifiable existing juristic person, to whom Personal Information may relate;

2.4. "**Data Breach**" means any unauthorised access to the Personal Information of Data Subjects in the possession or under the control of the Company or an Operator used by the Company;

2.5. "**Employee(s)**" all professionals and support staff members of the Company who may engage in or facilitate the Processing of Personal Information;

2.6. "**Information Officer**" means the individual appointed by the Company to maintain the privacy and protection of Personal Information in terms of a duly executed letter of appointment, and any reference to "**Information Officer**" shall also constitute a reference to a duly appointed "**deputy information officer**" as contemplated in terms of POPIA;

2.7. "**Information Regulator**" means the statutory body that is responsible for the enforcement and implementation of POPIA and which has been bestowed with extensive powers in terms of the Act, including the power to receive and investigate complaints, impose sanctions and publish guidelines and guidance documents in terms of POPIA compliance requirements;

2.8. "**Operator**" any person or entity that Processes Personal Information on behalf of a Responsible Party in terms of a contract or mandate, without falling under the direct authority of the Responsible Party;

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

2.10. "**Personal Information**" means any information relating to an identifiable, living natural person and if applicable, to an existing identifiable juristic person, including –

2.10.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, sexual orientation, age, physical or mental health, wellbeing, disability, religion, belief, culture, language and place of birth of the person;

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

2.10.3. an identifying number, symbol, e-mail address, telephone number, location, online identifier or other particular assignment to the person;

2.10.4. the biometric information of the person;

2.10.5. the personal opinions, views or preferences of the person or the views or opinions of another individual about the person;

2.10.6. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal contents of the original correspondence; and

2.10.7. 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;

2.11. "**POPIA / the Act**" means the Protection of Personal Information Act 4 of 2013, as amended, substituted or varied from time to time;

2.12. "**Policy"** means this information protection policy, as amended from time to time, including the appendices attached hereto;

2.13. "**Processing**" means the processing of Personal Information involves any collection, use, storage, deletion or destruction of Personal Information. The processing of Personal Information is of an ongoing nature and compliance with the provisions of POPIA must be in place for as long as the Personal Information is being processed and stored, and "**Process**" and "**Processed**" in this context shall have a corresponding meaning;

2.14. "**Records**" means any recorded information—

2.14.1. regardless of form or medium, including any of the following:

2.14.1.1. Writing on any material;

2.14.1.2. 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;

2.14.1.3. label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

2.14.1.4. book, map, plan, graph or drawing;

2.14.1.5. 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;

2.14.2. in the possession or under the control of a responsible party;

2.14.3. whether or not it was created by a responsible party; and

2.14.4. regardless of when it came into existence

2.15. "**Responsible Party**" means the party responsible for ensuring compliance with POPIA when Processing Personal Information, and encompasses any public or private bodies or any other

person that either alone or together with others, determines the purpose of and means for Processing Personal Information, and "Responsible Parties" shall have a corresponding meaning;

2.16. "**Special Personal Information**" means Personal Information concerning –

2.16.1. The religious or philosophical beliefs;

2.16.2. race or ethnic origin;

2.16.3. trade union membership;

2.16.4. political persuasion;

2.16.5. health or sex life; or

2.16.6. biometric information (which includes information that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition),

of a Data Subject; or

2.16.7. the criminal behaviour of a Data Subject to the extent that such information relates to –

2.16.7.1. the alleged commission by a Data Subject of any offence; or

2.16.7.2. any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings;

2.17. **"Technical and Organisational Security Measures**" means those appropriate, reasonable, technical and organisational measures aimed at protecting the integrity and confidentiality of Personal Information against loss of, damage to or unauthorised destruction and unlawful access to and against all other unlawful forms of Processing, and includes any generally accepted information security practices and procedures which may apply generally or be required in terms of specific industry or professional rules and regulations.

3. SCOPE

3.1. This Policy applies to all our Employees (including temporary, fixed-term, and permanent employees), consultants, contractors, trainees, seconded staff, home workers, casual workers, agency staff, volunteers, interns, agents, sponsors, or any other person or persons associated with us (including third parties), no matter where they are located. The Policy also applies to all directors, board members, and/or shareholders at any level.

3.2. This Policy –

3.2.1. sets out the minimum standards to which all Employees of the Company must adhere to at all times;

3.2.2. exists in order to set out the responsibilities of all parties to whom this Policy applies;

3.2.3. serves as a source of information and guidance for those to whom it applies on how to deal with the Processing of Personal Information; and

3.2.4. provide information and guidance on how to deal with a Data Breach.

4. DATA COLLECTION FRAMEKWORK AND COMPLIANCE

POPIA makes provision for eight pillars, which govern the lawful Processing of Personal Information.

As a Responsible Party, these so-called pillars of compliance must be adhered to by the Company in order to ensure that we successfully discharge our obligations in terms of POPIA and lawfully Process Personal Information. Our approach to ensuring compliance with our obligations under each condition is set out more comprehensively below.

PILLARS	COMPLIANCE DUTY	APPLICABLE SECTIONS OF CHAPTER 3 OF POPIA
1	Accountability	8
2	Processing limitation	9, 10, 11, 12
3	Purpose specification	13, 14
4	Further Processing limitation	15
5	Information quality	16
6	Openness	17, 18
7	Security safeguards	19, 20, 21, 22
8	Data Subject participation	23, 24, 25

4.1. **PILLAR 1: Ensuring accountability**

4.1.1. The Company must ensure that the conditions set out in POPIA are complied with at the time of the determination of the purpose and means of processing as well as during Processing itself.

4.1.2. *Internal Accountability*

4.1.2.1. The Company endorses a policy of responsibility, not only by the Company to Data Subjects but also by Employees to the Company.

4.1.2.2. Employees must keep in mind that the Company is accountable in terms of POPIA when we Process any Personal Information as a Responsible Party. Therefore, care should always be taken by all Employees when dealing with Personal Information.

4.1.2.3. In the event that any Employee is uncertain of our POPIA obligations when dealing with Personal Information internally, same should be discussed with the Information Officer without delay.

4.1.3. *Accountability when outsourcing Processing of Personal Information*

4.1.3.1. Responsible Parties will often, for a variety of reasons, wish to share Personal Information under their possession and control with third parties. For example, Responsible Parties may want to share Personal Information for certain operational reasons, between their related and inter-related business entities. Such sharing of Personal Information may be rendered POPIA compliant if the Data Subject is informed of this fact and consents to the sharing of their Personal Information.

4.1.3.2. Responsible Parties may also wish to outsource the Processing of Personal Information to third party operators who further Process the Personal Information on behalf of the Responsible Party for the payment of a fee. Operators generally include, amongst others, various service providers, businesses such as payroll companies, telemarketing companies or businesses that conduct customer satisfaction surveys, process research data or store and administer information.

4.1.3.3. The sharing of Personal Information with Operators is permissible provided that all the requirements for outsourcing of the Personal Information to an Operator in terms of POPIA are met.

4.1.3.4. The outsourcing of Personal Information to an Operator does not release the Responsible Party from its obligations in terms of POPIA. If the Operator contravenes POPIA in any way, the Responsible Party will still be held accountable.

4.1.3.5. In order to ensure that the principle of accountability is adhered to, the following measures will be taken when Operators Process Personal Information on behalf of the Company:

4.1.3.5.1. All contracts with Operators should include clauses which require the Operator to make use of security safeguards that measure up to or surpass the standards used by the Company and those required in terms of POPIA.

4.1.3.5.2. Provision should be made in all Operator agreements for the Operator to be held liable for damages suffered if a claim for a Data Breach is successful against the Company.

4.2. **PILLAR 2: Limiting the Processing of Personal Information**

4.2.1. The Processing Limitation condition entails that the Company –

4.2.1.1. should only allow minimal Processing of Personal Information;

4.2.1.2. should obtain the consent of Data Subjects in order to Process Personal Information;

4.2.1.3. must be justified in Processing the Personal Information; and

4.2.1.4. should as far as is reasonably practicable, collect Personal Information directly from the particular Data Subject.

4.2.2. *Lawful processing*

4.2.2.1. As a general rule, all Personal Information Processed by Employees must be treated as sensitive information and must not be disseminated or discussed with parties not involved in the Processing. More comprehensive detail relating to which Employees are permitted to have access to which type of information is set out in "**Annexure A**" (Data Subject Access to Information Policy) hereto.

4.2.3. *Minimality*

4.2.3.1. The Personal Information which is being Processed should not be excessive. Only the necessary and required Personal Information should be Processed to achieve the goal for which it is Processed.

4.2.4. *Consent, justification and objection*

4.2.4.1. Processing Personal Information should only commence once consent is received from the Data Subject to Process their information, where the Data Subject is a minor, a competent person should consent on their behalf.

4.2.4.2. The consent of the Data Subject is not required in the following circumstances:

4.2.4.2.1. when the Processing occurs in the process of carrying out obligations in terms of a contract to which the Data Subject is a party;

4.2.4.2.2. when the Processing is conducted by the Company to meet a statutory obligation;

4.2.4.2.3. where the Processing protects a legitimate interest of the Data Subject; or

4.2.4.2.4. when Processing is necessary to pursue the interests of the Company or a third party to whom the Personal Information is supplied.

4.2.4.3. Adequate records should be kept by the Employee who obtained consent from the Data Subject to prove that consent for the Processing was indeed obtained. These records should be stored in hard copy on the physical file (if applicable) and an electronic version on the electronic platforms used by the Company.

4.2.4.4. While practical measures to prove consent may vary from time to time, the signed client customers received from customers is sufficient consent to Process their Personal Information in line with their instructions.

4.2.5. *Collection directly from Data Subject*

4.2.5.1. Personal Information should always be collected directly from the Data Subject as far as possible. The following circumstances are exceptions to this rule:

4.2.5.1.1. The Personal Information is available in or collected from a public record or has been deliberately been made public by the Data Subject.

4.2.5.1.2. Either the Data Subject or a competent person on behalf of the Data Subject has consented to the collection of their Personal Information from another source.

4.2.5.1.3. The legitimate interests of the Data Subject would not be prejudiced by collection from another source.

4.2.5.1.4. When collection from another source is necessary –

4.2.5.1.4.1. for the Company to meet a statutory obligation;

4.2.5.1.4.2. to maintain the legitimate interests of the Company or a third party to whom the Personal Information is supplied; and

4.2.5.1.4.3. for use in court or tribunal proceedings (such as arbitration) that have either already commenced or are reasonably being contemplated.

4.2.5.1.5. The lawful purpose of collecting the Personal Information would be prejudiced by collecting directly from the Data Subject.

4.2.5.1.6. Collection directly from the Data Subject is not reasonably practicable in any particular case.

4.2.5.2. Where collection from any source other than the Data Subject directly is contemplated, such collection should be approved by the relevant Employee in writing, to be kept on record, setting out why collection from the Data Subject was not appropriate in the particular circumstances. In the event that an Employee has any uncertainty regarding the collection of any information from a source other than the Data Subject, this should be brought to the attention of and discussed with the Information Officer without delay.

4.3. **PILLAR 3: Processing Personal Information in line with its purpose**

4.3.1. POPIA requires that Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company.

4.3.2. *Collection for specific purpose*

4.3.2.1. Any Personal Information collected must be collected for a specific purpose and be related to a function or activity that is performed by the Company. This will substantially differ from case to case, however the provisions of this Policy and relevant legislation should be used as guide to determine to what extent Personal Information is necessary to achieve the desired outcome for any matter.

4.3.2.2. The Data Subject should therefore be informed of what the purpose for the Processing of their Personal Information is.

4.3.3. *Retention and restriction of records*

4.3.3.1. POPIA requires that once the purpose for which the Personal Information was collected has been achieved, it should no longer be retained. Though this is a general requirement, the nature of the work that the Company engages in means that retention of records for varying periods of time remains essential. The retention, restriction and deletion of records is set out in "**Annexure E**" (Retention of Personal Information Policy).

4.4. **PILLAR 4: Further Processing to be done in line with its original purpose**

4.4.1. Any further Processing of Personal Information in the possession of the Company must be Processed in accordance or compatible with the purpose for which it was originally collected. The further Processing of Personal Information should take into account –

4.4.1.1. the relationship between the purpose of the intended further Processing and the purpose for which the information was originally collected;

4.4.1.2. the nature of the Personal Information concerned;

4.4.1.3. the consequences, if any for the Data Subject due to the further Processing;

4.4.1.4. the manner that the Personal Information was initially collected; and

4.4.1.5. any contractual obligations and rights between the Data Subject and the Company.

4.4.2. The further Processing is compatible with the original purpose if –

4.4.2.1. consent for such Processing has been obtained from either the Data Subject or a competent person, in the case of a minor;

4.4.2.2. the Personal Information is available in or collected from a public record or has been deliberately been made public by the Data Subject; and/or

4.4.2.3. the further Processing is needed for –

4.4.2.3.1. compliance with any statutory duty; and

4.4.2.3.2. for use in court or tribunal proceedings that have either already commenced or are reasonably being contemplated.

4.4.3. The further Processing of Personal Information may also take place under such exceptions as published by the Information Regulator from time to time pursuant to section 37 of POPIA

4.4.4. If the Personal Information collected will be used for any purpose other than the original purpose, the relevant Employee must first obtain consent from the Data Subject prior to such Processing, or such Processing must otherwise be justified.

4.5. **PILLAR 5: Ensuring the quality of Personal Information**

4.5.1. POPIA places a duty on the Company to put in place reasonably practicable measures that Personal Information Processed by the company is complete, accurate and updated where necessary. To this end, the following is expected of Employees:

4.5.1.1. Where any matter, relationship or transaction continues over a period of time exceeding 12 (TWELVE) months, the Data Subject should be contacted to confirm the continued accuracy and comprehensive nature of information in possession of the Company.

4.5.1.2. Should the responsible Employee have any reason to reasonably suspect that the information in possession of the Company is incorrect or outdated, the Employee must contact the Data Subject to ascertain the accuracy of the Personal Information.

4.5.1.3. The purpose of the Personal Information in possession of the Company should be taken into consideration when considering the above, if a particular matter requires more frequent confirmation of such information, the Employee should undertake such follow ups with due care and as often as may be necessary in the circumstances.

4.5.2. In the event that an Employee has any uncertainty regarding data quality and their obligations in this regard, this should be brought to the attention of and discussed with the Information Officer without delay.

4.6. **PILLAR 6: Ensuring transparency and openness**

4.6.1. The purpose of the collection of the Data Subject's Personal Information must be transparent. This goal is advanced through the condition of “openness” which, in essence, requires that Data Subjects must be notified when their Personal Information is being Processed.

4.6.2. The Employee handling the Processing of the Personal Information must follow the internal procedures, set out in the Compliance Framework to ensure that the Data Subject is aware that their Personal Information is being Processed by the Company.

4.6.3. Records must also be kept all employees of all Processing activities conducted by them in relation to a particular Data Subject.

4.6.4. *Documentation*

4.6.4.1. POPIA requires that the Company retain documentation to prove the Processing of all Personal Information that the Company Processes. These records must be stored

in electronic and where applicable, physical files relating to the relationship between the Company and the Data Subject involved, where applicable.

4.6.5. *Notification to Data Subject when collecting Personal Information*

4.6.5.1. The following practical measures are to be put in place to ensure that Data Subjects are informed that the Company is Processing their Personal Information, to the extent that such Processing is not otherwise justified in terms of POPIA and notification is not required:

4.6.5.1.1. The Data Subject should be notified, through an electronic mail or otherwise, prior to the collection of Personal Information, that the Company is Processing their Personal Information and should be given a link or document indicating the following –

4.6.5.1.1.1. the Personal Information being collected and where the information is not collected from the Data Subject, the source from which it is collected;

4.6.5.1.1.2. the name and address of the Company;

4.6.5.1.1.3. the purpose for which the Personal Information is being collected;

4.6.5.1.1.4. whether the supply of the Personal Information by that data subject is voluntary or mandatory;

4.6.5.1.1.5. the consequences of failure to provide the Personal Information;

4.6.5.1.1.6. any particular law authorising or requiring the collection of the Personal Information, such as, for example, the Financial Intelligence Centre Act 38 of 2001;

4.6.5.1.1.7. if applicable, that the Company intends to transfer the Personal Information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

4.6.5.1.1.8. any further relevant information, such as the—

4.6.5.1.1.8.1. recipient or category of recipients of the Personal Information;

4.6.5.1.1.8.2. nature or category of the Personal Information;

4.6.5.1.1.8.3. existence of the right of access to and the right to rectify the Personal Information collected;

4.6.5.1.1.8.4. existence of the right to object to the Processing of Personal Information; and

4.6.5.1.1.8.5. right to lodge a complaint to the Information Regulator.

4.6.5.1.2. In any matter where the collection does not take place directly from the Data Subject, the Data Subject should be notified prior to the collection of their Personal Information and where this is not reasonably practicable, as soon as possible thereafter, provided that the Processing of Personal Information is otherwise justified in terms of POPIA.

4.6.5.1.3. Notification as set out in paragraph 4.6.5.1.2 is not necessary if:

4.6.5.1.3.1. the Data Subject or competent person, in the case of a minor, has consented to and indicated that such notification is not required;

4.6.5.1.3.2. non-compliance will not negatively prejudice the legitimate interests of the Data Subject as set out in POPIA and this Policy;

4.6.5.1.3.3. the notification is prevented by any legislation;

4.6.5.1.3.4. the Personal Information collected is for use in court or tribunal proceedings that have either already commenced or are reasonably being contemplated;

4.6.5.1.3.5. compliance would prejudice a lawful purpose of the collection;

4.6.5.1.3.6. the circumstances of a particular matter render such notification reasonably impracticable; or

4.6.5.1.3.7. the information collected will be used in such a way that the Data Subject cannot be identified or will be used for historical, statistical or research purposes.

4.7. **PILLAR 7: Ensuring the implementation of security safeguards**

4.7.1. Personal Information collected from a Data Subject must be securely. The integrity of all Personal Information must be maintained through all technical and organisational measures and/or Processes to prevent the loss of, damage to, unauthorised destruction of, unlawful access to or the unlawful Processing of Personal Information.

4.7.2. *Security measures on integrity and confidentiality of Personal Information*

4.7.2.1. In order to ensure that all Personal Information Processed by the Company is kept secure, Personal Information must be Processed and particular focus is placed on the storage in compliance with the appropriate security measures as set out in "**Annexure F**" (Data Security Policy).

4.7.2.2. With the aim of strengthening compliance with the provisions of POPIA, annual audits will be conducted to ensure that the security measures as set out in "**Annexure F**" (Data Security Policy).

4.7.3. *Information processed by an Operator or person acting under authority*

4.7.3.1. Where an Operator Processes Personal Information on behalf of the Company, the following provisions must be included in any agreement to conduct such Processing:

4.7.3.1.1. the Operator must inform the Company when Processing of such Personal Information occurs; and

4.7.3.1.2. measures should be included in all agreements to conduct such Processing to safeguard the confidentiality of such Personal Information.

4.7.4. *Security measures regarding Personal Information processed by Operator*

4.7.4.1. All contracts with Operators should include clauses which require the Operator to make use of security safeguards that measure up to or surpass the standards used by the Company.

4.7.4.2. The Operator should be required in terms of such agreement to notify the Company immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.

4.7.4.3. Provision should be made in all operator agreements for the Operator to be held liable for damages suffered if a claim for a Data Breach is successful against the Company.

4.7.5. *Notification of security compromises*

4.7.5.1. Notification in the event of a Data Breach is mandated by POPIA, the specifics of the internal procedure to follow in the case of a Data Breach is set out in "**Annexure G**" (Data Breach Policy) and **"Annexure H"** (Data Breach Report Form).

4.8. **PILLAR 8: Enabling Data Subject participation**

4.8.1. The Data Subject has the right to request and to find out whether the Company holds their Personal Information and a description of the Personal Information so held. The data subject has a further right to request the responsible party to correct or update the personal information as well as destroy the record and the responsible party must act upon such request by the data subject.

4.8.2. *Access to personal information*

4.8.2.1. Section 23 of the Act requires that procedures be put in place by the Company to enable Data Subjects who have provided adequate proof of identity to request access to their Personal Information. The request for access to records is set out in **"Annexure C"** (Request for Access to Record of Private Body Form).

4.8.3. *Correction of personal information*

4.8.3.1. Section 24 of the Act requires that procedures be put in place by the Company to enable Data Subjects who have provided adequate proof of identity to request the correction or amendment of their Personal Information, which is in the possession of the Company. The request to amend personal information is set out in **"Annexure D"** (Request for Correction or Deletion Form).

4.8.4. *Manner of access*

4.8.4.1. Section 25 of the Act requires the Data Subject to elect the manner in which the decision of their request is communicated to the Data Subject. The is set out in **"Annexure C"** (Request for Access to Record of Private Body Form).

4.9. In the event that an Employee has any uncertainty regarding any of the above provisions or the processing of the Personal Information, this should be brought to the attention of and discussed with the Information Officer without delay.

5. EMPLOYEE RESPONSIBILITIES

5.1. All our Employees are responsible for ensuring that they read and understand this Policy. In addition, compliance with this Policy and its contents are expected of all our Employees.

5.2. All Employees may be required to attend training in relation to this Policy.

5.3. All Employees under our control are equally responsible for the Processing of Personal Information in line with this Policy and are required to avoid any and all activities that could lead to, or imply, a breach of this Policy.

5.4. Where an employee performs work in different jurisdictions, the employee is expected to comply with the requirements of the respective jurisdictions which laws are applicable at any given moment in time.

5.5. The duty of Employees to report suspicious activities includes the duty to report if they have a reasonable suspicion that a Data Breach may have occurred, is in the process of occurring, or may occur in future.

6. INTERNAL PROCEDURES TO RAISE CONCERNS

6.1. The internal procedures to raise concerns are not set out in detail in this Policy, however any employee who wishes to raise a concern should first contact their line manager and inform them of the circumstances.

6.2. Should the line manager fail to take action or fail to take appropriate action, the employee may approach the Information Officer for this Policy directly to raise their concern in a more formal manner.

6.3. Any person or employee who does raise such a concern shall not be identified to fellow employees and shall be afforded all reasonable protection of their privacy to prevent problems in the workplace.

7. BREACH OF THIS POLICY

7.1. Compliance with the provisions of this Policy is mandatory and failure to do so can result in severe consequences for the Company and the individuals concerned. Failure to comply with this Policy may lead to Employees being subject to disciplinary action, up to and including dismissal.

8. MONITORING OF COMPLIANCE

8.1. We recognise that as time passes changes may become necessary to ensure that this Policy remains effective and up to date. The Information Officer is authorised in terms of this Policy to, from time to time, conduct internal audits and compliance assessments across all business areas of the Company, in order to –

8.1.1. establish the compliance status of the Company in terms of the Act

8.1.2. adherence by Employees to this Policy;

8.1.3. confirm adequate recordkeeping of Personal Information documentation by the Company; and

8.1.4. identify training and support needs of Employees in respect of this Policy.

8.2. Such audit and compliance assessments reports will be submitted to Senior Management for consideration, and must include suggested remedial measures by the Company for the correction of any identified compliance shortfalls or gaps and recommendations for the improvement of the Compliance Framework of the Company.

8.3. Should any need for improvements or adjustments arise, they will be implemented as soon as is reasonably possible and has been approved by the Senior Management of the Company.

ANNEXURE A: DATA SUBJECT ACCESS TO INFORMATION POLICY

Both POPIA and PAIA regulate the data's subject access to information as well as the data subject's right to participate.

1. CATEGORY OF INFORMATION:

For the purposes of the Processing of Personal Information within the Company, there are generally 3 (THREE) categories, namely information relating to customers, Employees and service providers.

1.1. CUSTOMERS

1.1.1. The Personal Information of all customers should be treated as confidential and should be Processed in compliance with the provisions of this Policy by all Employees.

1.1.2. Any queries relating to the Processing of customers' Personal Information should be directed to the Information Officer.

1.2. EMPLOYEES

1.2.1. The Personal Information of all Employees shall be treated as confidential, and should be Processed in compliance with the provisions of this Policy by all Employees.

1.2.2. Access to the Personal Information of fellow Employees, except as is generally available and known to Employees in the course and scope of their employment, is generally not permitted, and any queries in this regard should be directed to the Human Resources Manager of the Company; the finance department or Senior Management.

1.3. SERVICE PROVIDERS

1.3.1. The Personal Information of all service providers shall be treated as confidential, and should be Processed in compliance with the provisions of this Policy by all Employees.

1.3.2. Any queries in this regard should be addressed to the Information Officer.

2. DATA SUBJECT ACCESS REQUEST

2.1. A data subject who wishes to request access to records of the Company and Personal

Information that the Company holds shall complete **"Annexure C"** (Request for Access to Record of Private Body Form).

2.2. A data subject who wishes to object to the processing of their personal information shall complete **"Annexure B"** (Objection to Processing of Personal Information Form).

2.3. A data subject who wishes to request the correction or deletion the Personal Information held by the Company shall complete **"Annexure D"** (Request for Correction or Deletion Form).

2.4. The Information Officer may request further information to clarify the Access Request Form or request proof of identification of the person making the request. but shall as far as possible, endeavour to comply with the request within a reasonable time.

3. GROUNDS FOR REFUSAL OF ACCESS TO CERTAIN RECORDS

3.1. Part 3, Chapter 4 of PAIA provides grounds that justify the Company's refusal to comply with a request to Personal Information. Such instances include mandatory protection of –

3.1.1. privacy of a third party who is natural person;

3.1.2. commercial information of a third party;

3.1.3. certain confidential information of a third party;

3.1.4. information relating to the safety of individuals, and protection of property;

3.1.5. records privileged from production in legal proceedings;

3.1.6. commercial information of a private body; and

3.1.7. research information of third parties, and protection of research information of private bodies.

3.2. Requests for records which are clearly frivolous, vexatious or involve an unreasonable diversion of resources may also be refused.

4. DECISION TO GRANT OR DENY ACCESS

4.1. Our Information Officer will deliberate and decide on the request of the Requester within 30 (thirty) days of receipt of the request for access.

4.2. In cases where the request for access is for a large number of records or the request requires a search at more than one of our offices the period may be extended for a further period of up to 30 (THIRTY) days.

5. FEES

5.1. Under normal circumstances, the Company does not normally charge for a request to only confirm whether the personal information of the data subject is kept by the Company.

5.2. It is permissible to charge a fee to cover the administrative costs of complying with a request for access to Personal Information or access to records of the Company in so far as it relates to the disclosure of Personal information processed by the Company.

5.3. In the event that the preparation of the records requested exceed 6 (SIX) hours, a deposit is payable equal to not more than one third of the access fees (which would be payable if the request were to be granted).

5.4. The following factors should be considered when calculating a reasonable fee:

5.4.1. Administrative costs involved in:

5.4.1.1. Assessing whether or not the Company is processing the data subject's information;

5.4.1.2. Locating, retrieving, and extracting that information;

5.4.1.3. Providing a copy of the information; and

5.4.1.4. Sending the Company's response to the data subject

5.4.2. Specific costs to be considered include:

5.4.2.1. Photocopying, printing, postage, and any other costs incurred when sending the information to the data subject;

5.4.2.2. Equipment and supplies; and

5.4.2.3. Staff time.

5.4.3. The fees are regulated in terms of the Regulations to PAIA that are updated from time to time.

6. REMEDIES FOR REFUSAL OF ACCESS TO INFORMATION REQUEST

6.1. Internal Appeal

6.1.1. The decision of the Information Officer or Deputy Information Officer is final in terms of our internal procedures for access to information. The external remedies set out below remain available to the Requester, however there is no internal appeal procedure.

6.2. External Appeal

6.2.1. The Requester may in terms of sections 56(3)(c) and 78 of PAIA apply to a court within 180 days of notification of the decision for appropriate relief.

ANNEXURE B: OBJECTION TO PROCESSING OF PERSONAL INFORMATION FORM

FORM 1
OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 2]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……...

.....
Signature of data subject/designated person

ANNEXURE C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY FORM

FORM C

REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))

[Regulation 7 of 2021]

A. Particulars of private body

The Head:

SUNGROW SOUTHERN AFRICA (PTY) LTD

1ST FLOOR WRIGLEY FIELD BUILDING

THE CAMPUS

57 SLOANE STREET

SANDTON, JOHANNESBURG

GAUTENG, SOUTH AFRICA

2191

B. Particulars of person requesting access to the record

(a) The particulars of the person who requests access to the record must be given below.
(b) The address and/or fax number in the Republic to which the information is to be sent must be given.
(c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname: …….

Identity number:……

Postal address: ……

Telephone number: (……) …… Fax number: (……)……..…

E-mail address: ……

Capacity in which request is made, when made on behalf of another person:

……

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname: ……

Identity number: ……..

D. Particulars of record

(a) Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.

(b) If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of record or relevant part of the record:

……

……

……

……

2. Reference number, if available:

……

……

……

……

3. Any further particulars of record:

……

……

……

……

E. Type of Record

(Mark the applicable box with "X")

Records is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

F. Form of Access

(Mark the applicable box with "X")

Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive *(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

G. Manner of Access

(Mark the applicable box with "X")

Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/ file transfer	
Preferred language: *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

H. Particulars of Right to be Exercised or Protected

If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.

1. Indicate which right is to be exercised or protected:

……
……
……
……

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

……
……
……
……

I. Fees

(a) A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b) You will be notified of the amount required to be paid as the request fee.
(c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.
(d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

……
……
……
……

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

Postal address	**Facsimile**	**Electronic communication** ***(Please specify)***

Signed at …… this day…… of ……..……year …….

……
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE

FOR OFFICIAL USE

Reference number:	
Request received by: (state rank, name and surname of information officer)	
Date received:	
Access fees:	
Deposit (if any):	

……
SIGNATURE OF INFORMATION OFFICER

ANNEXURE D: REQUEST FOR CORRECTION OR DELETION FORM

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	

Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20……...

.....
Signature of data subject/ designated person

ANNEXURE E: RETENTION OF PERSONAL INFORMATION POLICY

1. Retention Of Personal Information

1.1. The general requirement under POPIA is that once the purpose for which the Personal Information was collected has been achieved, it should no longer be retained. However, the nature of the work that the Company engages in means that retention of records for varying periods of time remains essential.

1.2. The following circumstances are exceptions that apply to such records and Personal Information, records may be retained if –

1.2.1. retention is required by law;

1.2.2. the Company requires the record for lawful purposes related to its functions and activities;

1.2.3. retention is agreed to in a contract between the Company and the Data Subject; or

1.2.4. where consent for such retention has been obtained from either the Data Subject or a competent person, in the case of a minor.

1.3. Where the Company has made use of the Personal Information to make a decision of the Data Subject –

1.3.1. the record must be retained as required by law or any applicable code of conduct; or

1.3.2. if such law or code of conduct is not applicable, records should be retained for a period sufficient to allow the Data Subject a reasonable opportunity to request access to the records in line with the POPIA compliant PAIA Manual.

1.4. Section 51 of the Electronic Communications Act requires that Personal Information and all documentation relating to its Processing is kept for a period of one year or for as long as such Personal Information is in use. For internal auditing requirements, this period is extended to five years from the date of the Personal Information's last Processing, unless otherwise agreed by the Data Subject at the date of the collection of such Personal Information or any subsequent date thereafter.

1.5. Once the circumstances contemplated above ceases to exist and the relevant period contemplated in paragraph 1.4 has expired, the records must be destroyed or deleted.

1.6. The destruction or deletion contemplated above should render the records unidentifiable and incapable or reconstruction.

2. Restriction Of Processing Personal Information

2.1. The Processing of Personal Information by the Company will be restricted if –

2.1.1. the accuracy of the Personal Information is contested by the Data Subject, this restriction will be applicable until the Company can verify the accuracy of the Personal Information;

2.1.2. the Company has achieved the purpose for which the Personal Information was initially collected and it is now merely retained for record keeping purposes;

2.1.3. the Processing took place in an unlawful manner. However, the Data Subject may request that the Personal Information not be deleted or destroyed and that its Processing be restricted instead; or

2.1.4. the Data Subject requests that the Personal Information be transferred to an alternative automated processing system.

2.2. The Personal Information identified in paragraph 3.1 may only be stored and not Processed further, unless it is Processed for –

2.2.1. purposes of proving any legitimate matter related to the initial purpose of the Processing by the Company;

2.2.2. a matter where consent for such Processing has been obtained from either the Data Subject or a competent person, in the case of a minor;

2.2.3. purposes of protecting the interests of another natural or legal person; or

2.2.4. the benefit of the public interest.

2.3. If the Processing of Personal Information is restricted in terms of the above, the Data Subject must be informed prior to the lifting of the restriction of the Processing of such information.

3. Disposal of Personal Information

3.1. Upon the expiry of the retention periods set out above, or when a data subject exercises their right to have their personal information erased, personal information shall be deleted, destroyed, or otherwise disposed of as follows:

3.1.1. Special personal information stored electronically (including any and all backups thereof) shall be deleted securely through a hard delete and complete deletion of the files from the system.

3.1.2. Special personal information stored in hardcopy form shall be shredded to at least 6 mm strips and recycled.

3.1.3. Personal information stored electronically (including any and all backups thereof) shall be deleted securely through a hard delete and complete deletion of the files from the system

3.1.4. Personal information stored in hardcopy form shall be shredded to at least 10 mm strips and recycled.

ANNEXURE F: DATA SECURITY POLICY

1. Introduction

1.1. This document sets out the measures to be taken by all employees of the Company and by the Company as a whole in order to protect data (electronic and otherwise) collected, held, and processed by the Company, and to protect the Company's computer systems, devices, infrastructure, computing environment, and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental.

2. Key Principles

2.1. All IT Systems and data are to be protected against unauthorised access.

2.2. All IT Systems and data are to be used only in compliance with relevant Company Policies.

2.3. All personal information must be used only in compliance with POPIA and the Company's Personal Information Protection Policy.

2.4. All employees of the Company and any and all third parties authorised to use the IT Systems and data collected, held, and processed by the Company including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy Page 2 of 11 and must adhere to and comply with it at all times.

2.5. All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.

2.6. All data must be classified appropriately (including, but not limited to, personal information, special personal information or confidential information). All data so classified must be handled appropriately in accordance with its classification.

2.7. All data, whether stored on IT Systems or in hardcopy format, shall be available only to those Users with a legitimate need for access.

2.8. All data, whether stored on IT Systems or in hardcopy format, shall be protected against unauthorised access and/or processing, ang against loss and/or corruption.

2.9. All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the "IT Department" or by such third party/parties as the IT Department may from time to time authorise.

2.10. The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the IT Department unless expressly stated otherwise.

2.11. The responsibility for the security and integrity of data that is not stored on the IT Systems lies with the Heads of Departments.

2.12. All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the IT Department. Any breach which is either known or suspected to involve personal information shall be reported to the Information Officer or any of the appointed Deputy Information Officers.

2.13. All breaches of security pertaining to data that is not stored on the IT Systems shall be reported and subsequently investigated by Heads of Departments. Any breach which is either known or suspected to involve personal information shall be reported to the Information Officer or any of the appointed Deputy Information Officers.

2.14. All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the IT Department. If any such concerns relate in any way to personal information, such concerns must also be reported to the Information Officer.

2.15. All Users must report any and all security concerns relating to data that is not stored on the IT Systems immediately to, the Head of the Department. If any such concerns relate in any way to personal information, such concerns must also be reported to the Information Page 3 of 11 Officer or any of the appointed Deputy Information Officers.

3. Department Responsibilities

3.1. The IT Manager shall be responsible for the following:

3.1.1. ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements;

3.1.2. ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Information Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management and the Information Officer;

3.1.3. ensuring that all Users are kept aware of the IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the POPIA.

3.2. The appointed Deputy Information Officers shall be responsible for the following:

3.2.1. ensuring that all other data processing systems and methods are assessed and deemed suitable for compliance with the Company's security requirements;

3.2.2. ensuring that data security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Information Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management and the Information Officer;

3.2.3. ensuring that all Users are kept aware of the non-IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, POPIA.

3.3. The IT Staff shall be responsible for the following:

3.3.1. assisting all Users in understanding and complying with the IT-related aspects of this Policy;

3.3.2. providing all Users with appropriate support and training in IT security matters and use of IT Systems;

3.3.3. ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

3.3.4. receiving and handling all reports relating to IT security matters and taking appropriate action in response including, in the event that any reports relate to personal information, informing the Information Officer;

3.3.5. taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

3.3.6. assisting the IT Manager in monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and

3.3.7. ensuring that regular backups are taken of all data stored within the IT Systems at intervals and such backups are stored at a suitable location onsite and/or offsite. All backups should be encrypted.

3.4. The Heads of Departments shall be responsible for the following:

3.4.1. assisting all Users in understanding and complying with the nonIT-related aspects of this Policy;

3.4.2. providing all Users with appropriate support and training in data security matters;

3.4.3. ensuring that all Users are granted levels of access to data that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

3.4.4. receiving and handling reports concerning non-IT-related data security matters and taking appropriate action in response including, in the event that any reports relate to personal information, informing the Information Officer or any of the appointed Deputy Information Officers;

3.4.5. taking proactive action, where possible, to establish and implement security procedures and raise User awareness; and

3.4.6. assisting the Information Officer and appointed Deputy Information Officers in monitoring data security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future.

4. Users' Responsibilities

4.1. All Users must always comply with all relevant parts of this Policy when using the IT Systems and data.

4.2. All Users must use the IT Systems and data only within the bounds of South African legislation and must not use the IT Systems or data for any purpose or activity which is likely to contravene any legislation or Company policy whether now or in the future in force.

4.3. Users must immediately inform the IT Department and/or Head of the Department and, where such concerns relate to personal information, the Information Officer or any of the appointed Deputy Information Officers of any and all security concerns relating to the IT Systems or data.

4.4. Users must immediately inform the IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.

4.5. Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

5.1. All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the discretion of the IT Department.

5.2. Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.

5.3. No Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software belonging to Users must be approved by the IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

5.4. All software will be installed onto the IT Systems by the IT Department unless an individual User is given written permission to do so by the IT Manager. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. Anti-Virus Security Measures

6.1. Most IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up to date with the latest software updates and definitions.

6.2. All IT Systems protected by anti-virus software will be subject to a full system scan in intervals as recommended by the IT Department.

6.3. All physical media (e.g., USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred.

6.4. Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g., shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate.

6.5. Where any virus is detected by a User this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device.

6.6. If any virus or other malware affects, is likely to affect, or is suspected to affect any personal information, in addition to the above, the issue must be reported immediately to the Information Officer or any of the appointed Deputy Information Officers.

6.7. Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a dismissible offence under the Company's disciplinary procedures.

7. Hardware Security Measures

7.1. Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.

7.2. All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climatecontrolled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Department.

7.3. No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the IT Manager. Under normal circumstances, whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Manager.

7.4. All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

7.5. All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises.

7.6. The IT Department shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled, and the corresponding data shall be kept on the asset register.

8. Organisational Security

8.1. All Users handling data (and in particular personal information) will be appropriately trained to do so and will be appropriately supervised.

8.2. All Users handling data (and in particular personal information) shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to such data, whether in the workplace or otherwise.

8.3. All Users handling personal information will be bound to do so in accordance with the principles of the POPIA and relevant Company policies.

8.4. No data, personal or otherwise, may be shared informally and if a User requires access to any data, personal or otherwise, that they do not already have access to, such access should be formally requested from the Head of the Department.

8.5. No data, personal or otherwise, may be transferred to any unauthorised User without the authorisation of the Head of the Department.

8.6. All data must be handled with care at all times and should not be left unattended or on view to unauthorised Users or other parties at any time.

9. Access Security and Passwords

9.1. Access privileges for all IT Systems and data shall be determined on the basis of Users' levels of authority within the Company and the requirements of their job roles. Users shall not be granted access to any IT Systems or data which are not reasonably required for the fulfilment of their job roles.

9.2. All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate and approve. Not all forms of biometric log-in are considered secure. Only those methods approved by the IT Department may be used.

9.3. All passwords must, where the software, computer, or device allows:

9.3.1. be at least 8 characters long;

9.3.2. contain a combination of upper- and lower-case letters, numbers and symbols;

9.3.3. be changed at least every 90 days;

9.3.4. be different from the previous password;

9.3.5. not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.); and

9.3.6. be created by individual Users.

9.4. Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including the IT Manager and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the IT Department and, where personal information could be accessed by an unauthorised individual, the Information Officer or any of the appointed Deputy Information Officers.

9.5. If a User forgets their password, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

9.6. Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g., in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see.

9.7. All IT Systems with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver.

9.8. Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Manager. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the IT Manager and, where such access renders personal information accessible by the outside party, the Information Officer or any of the appointed Deputy Information Officers.

10. Data Storage Security

10.1. All data stored in electronic form, and in particular personal information, should be stored securely using passwords and data encryption.

10.2. All data stored in hardcopy format or electronically on removable physical media, and in particular personal information, should be stored securely in a locked box, drawer, cabinet, or similar.

10.3. No data, and in particular personal information, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-

contractor working on behalf of the Company and that User has agreed to comply fully with the Company's Data Protection Policy and POPIA.

10.4. No data, and in particular personal information, should be transferred to any computer or device personally belonging to a User that is an employee, unless written permission has been granted by the Head of Department and the Information Officer, and subject to the requirements pertaining to Data Security as set out in this policy as well as the Company's Data Protection Policy

11. Protection of Personal Information

11.1. All Users handling personal information for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Protection of Personal Information Policy at all times. In particular, the following shall apply:

11.1.1. All emails containing personal information must be encrypted;

11.1.2. Personal information may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

11.1.3. Personal information may not be transmitted over public wireless networks;

11.1.4. All personal information to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".

11.1.5. Where any personal information and/or other data covered by this Policy is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.

12. Internet and Email Use

12.1. All Users shall be subject to, and must comply with, the provisions of relevant Company policies pertaining to Communications, Email and Internet when using the IT Systems.

12.2. Where provisions in this Policy require any additional steps to be taken to ensure security when using the internet or email over and above the requirements imposed by other policies, Users must take such steps as required.

13. Reporting Security Breaches

13.1. All security breaches, whether relating to personal information or not, shall be dealt with in accordance with the Company's Data Breach Policy.

ANNEXURE G: DATA BREACH POLICY

1. Data Breaches

1.1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes and/or any other type of breach of personal information as recognised under POPIA.

1.2. Incidents to which this Policy applies may include, but not be limited to:

1.2.1. Loss or theft of personal data and/or equipment on which data is stored;
1.2.2. Access by an unauthorised third party;
1.2.3. Deliberate or accidental action (or inaction) by a controller or processor;
1.2.4. Sending personal data to an incorrect recipient;
1.2.5. Computing devices containing personal data being lost or stolen;
1.2.6. Alteration of personal data without permission;
1.2.7. Loss of availability of personal data;
1.2.8. Hacking attack;
1.2.9. Cyber attack;
1.2.10. Equipment failure;
1.2.11. Human error;
1.2.12. Unforeseen circumstances such as a fire or flood;
1.2.13. Flawed data destruction procedures.

2. Internal Reporting

2.1. If a data breach is discovered or suspected, members of staff should complete **"Annexure H"** (Data Breach Report Form) and send the completed form to the Company's Information Officer.

2.2. Where appropriate, members of staff should liaise with their direct line manager when completing a Data Breach Report Form.

2.3. If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable.

2.4. Unless and until instructed to by the Company's Information, members of staff should not take any further action with respect to a data breach. In particular, individual members of staff

should not take it upon themselves to notify affected data subjects, the Information Regulator, or any other individuals or organisations.

3. Initial Management and Recording

3.1. Upon receipt of an **"Annexure H"** (Data Breach Report Form) (or upon being notified of a data breach in any other way), the Company's Information Officer shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.

3.2. Having established the above, the following steps shall then be taken with respect to the data breach:

3.2.1. undertake an initial assessment of the data breach, liaising with the relevant staff and departments where appropriate, to establish the severity of the data breach;

3.2.2. contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;

3.2.3. determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;

3.2.4. establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;

3.2.5. determine, in liaison with the relevant staff and departments, the best course of action to resolve and remedy the data breach; and

3.2.6. record the breach and the initial steps taken above in the Company's Data Breach Register.

3.3. Having completed the initial steps described above, the Company's Information Officer shall proceed with investigating and assessing the data breach as described in Part 6, below.

4. Investigation and Assessment

4.1. The Company's Information Officer shall begin an investigation of a data breach as soon as is reasonably possible after receiving an "**Annexure H"** Data Breach Report Form (or being notified in any other way) and, in any event, within 24 hours of the data breach being discovered and/or reported.

4.2. Investigations and assessments must take the following into account:

4.2.1. the type(s) of data involved (and, in particular, whether the data is personal information or special personal information);

4.2.2. the sensitivity of the data (both commercially and personally);

4.2.3. what the data breach involved;

4.2.4. what organisational and technical measures were in place to protect the data;

4.2.5. what might be done with the data as a result of a breach (including unlawful or otherwise inappropriate misuse);

4.2.6. where personal information is involved, what that personal information could tell a third party about the data subjects to whom the data relates –

4.2.6.1. the category or categories of data subject to whom any personal information relates;

4.2.6.2. the number of data subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;

4.2.6.3. the potential effects on the data subjects involved;

4.2.6.4. the potential consequences for the Company;

4.2.6.5. the broader consequences of the data breach, both for data subjects and for the Company;

4.2.6.6. measures that can be taken to prevent similar data breaches.

4.3. The results of the investigation and assessment described above must be recorded in the Company's Data Breach Register.

4.4. Having completed the investigation and assessment described above, the Company's Information Officer and/or appointed Deputy Information Officers shall determine the parties to be notified of the breach as described in Part 7, below.

5. Notification

5.1. The Company's Information Officer shall determine whether to notify one or more of the following parties of the breach:

5.1.1. affected data subjects;

5.1.2. the Information Regulator;

5.1.3. the police;

5.1.4. the Company's insurers;

5.1.5. affected commercial partners;

5.2. When considering whether and how to notify the Information Regulator and individual data subjects in the event of a personal information breach, it must be considered whether such notification will interfere with a criminal investigation. In this regard guidance is to be sought from a public body responsible for the prevention, detection or investigation of offences, relevant to the data breach. Alternatively, it may be determined by the Information Regulator whether notification will impede a criminal investigation by the public body concerned.

5.3. When individual data subjects are to be informed of a data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

5.3.1. a user-friendly description of the data breach, including how and when it occurred, the personal information involved, and the likely consequences;

5.3.2. clear and specific advice, where relevant, on the steps individuals can take to protect themselves;

5.3.3. a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;

5.3.4. contact details for the Company's Information Officer from whom affected individuals can obtain further information about the data breach.

5.4. If the Information Regulator is to be notified of a significant breach of personal information within 72 hours, excluding weekends and public holidays, of becoming aware of the breach,

where feasible. This time limit applies even if complete details of the data breach are not yet available. The Information Regulator must be provided with the following information:

5.4.1. the category or categories and the approximate number of data subjects whose personal information is affected by the data breach;

5.4.2. the category or categories and the approximate number of personal information records involved;

5.4.3. the name and contact details of the Company's Information Officer from which the Information Regulator can obtain further information about the data breach;

5.4.4. a description of the likely consequences of the data breach; and

5.4.5. description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

5.5. Records must be kept of all data breaches, regardless of whether notification is required to the Information Regulator. The decisionmaking process surrounding notification should be documented and recorded in the Company's Data Breach Register.

6. Evaluation and Response

6.1. When the steps set out above have been completed, the data breach has been contained, and all necessary parties notified, the Company's Information Officer shall conduct a complete review of the causes of the data breach, the effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future.

6.2. Such reviews shall, in particular, consider the following with respect to data (and in particular, personal information) collected, held, and processed by the Company:

6.2.1. where and how data is held and stored;

6.2.2. the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;

6.2.3. the methods of data transmission for both physical and electronic data and whether or not such methods are secure;

6.2.4. the level of data sharing that takes place and whether or not that level is necessary;

6.2.5. whether any data protection impact assessments need to be conducted or updated;

6.2.6. staff awareness and training concerning data protection;

6.2.7. whether disciplinary action is to be instituted against any employee whose actions, whether directly or indirectly, resulted in the data breach.

6.3. Where possible improvements and/or other changes are identified, the Company's Information Officer shall liaise with relevant staff and/or departments with respect to the implementation of such improvements and/or changes.

ANNEXURE H: DATA BREACH REPORT FORM

SUNGROW SOUTHERN AFRICA (PTY) LTD

DATA BREACH REPORT FORM

Your Details

[NOTE: You may complete and submit this form anonymously. If you wish to do so, please put anonymous in each of the fields in this section. Please note that if you are submitting this form anonymously, you should not email it as this may identify you.]

Title:	
First Name(s):	
Surname:	
Department (if applicable):	
Manager/ supervisor:	
Contact Number:	
Email Address:	

Date of this Breach Report	

Details of Data Breach

Please provide as much detail as you can about the data breach that you have discovered or suspect. The more accurate and specific the information provided in this form, the more quickly and effectively the Company will be able to deal with the data breach.

Date and time of data breach:	
Date and time data breach	

discovered:	
Is the data breach actual or suspected?	
Please provide a summary of the data breach:	
What type(s) of data are involved?	
Approximately how much data is involved?	
Is personal information involved?	
Is special personal information involved?	
If personal (or special personal) information is involved, what type(s) of information subject are affected (e.g. customers, employees)? (please do not identify any individual data subjects)	
Approximately how many data subjects (if any) are likely to be affected (if known)? (please do not identify any individual data subjects)	
What caused the data breach? (please provide as much detail as you can)	

Have you or any other member of staff taken any action relating to the breach since discovery other than completing this form? (if yes, please provide as much detail as you can)	
Is the data breach ongoing?	
Are you aware of any other data breaches, related or otherwise? (if yes, please provide details)	

For Use by the Information Officer:

Received by:	
Date received:	
Forwarded for action to (if applicable):	
Date forwarded (if applicable):	