PROTECTION OF PERSONAL INFORMATION ("POPI") AND THE RETENTION OF DOCUMENTS:

POLICY FOR

GREENACRES HOLDINGS (PTY) LTD AND

ALL OF ITS SUBSIDIARIES RELATING TO:

CUSTOMER PERSONAL INFORMATION

Author: DG/Legal & Compliance

Version 1: October 2021

1. INTRODUCTION

1.1 **POPI** is the abbreviated term for the **PROTECTION OF PERSONAL INFORMATION ACT** ("the Act").The Act is distinguished from other similar pieces of legislation worldwide because the "personal information" as defined in the Act refers to **ANY information RELATING TO AN IDENTIFIABLE, LIVING NATURAL PERSON OR JURISTIC PERSON.** This means that there is not only a requirement to safeguard the personal information of an individual but that of customers and suppliers as well;

1.2 POPI therefore requires that the Greenacres Group of Companies ("the Group") inform their customers as to the manner in which their personal information is used, disclosed and destroyed and commits to customers that their privacy will be protected by ensuring that their personal information is used in an appropriate and secure manner in accordance with applicable laws;

1.3 Whilst the Act is a South African piece of legislation, the implementation of the provisions of this Act to all Group Companies including subsidiaries in Africa will be followed to the extent that such provisions do not contradict prevailing legislation in those African jurisdictions;

1.4 This policy is available on the Group's website and by request from the Group Legal & Compliance Department at Greenacres Holdings (Pty) Ltd.

2. COLLECTION OF PERSONAL INFORMATION

2.1 The Act provides that personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

2.2 In this regard, the Group collects and processes the personal information of its customers for the purposes of:

- *assessing the creditworthiness (credit reference searches and verifications) of the customer in the provision of incidental credit;*
- *using such information for the development of payment services from customers;*
- *conducting due diligences on the customer with reference to complying with the Group's policies relating to fraud, crime, money laundering, anti-trust, anti-bribery and corruption and sanction listed companies internationally;*
- *Marketing purposes in print and digital media;*
- *Confirming and verifying their details on record;*
- *For record and audit purposes;*
- *In connection with and complying with legal and statutory requirements or otherwise allowed by law;*
- *Necessary for pursuing the legitimate interests of the Group and/or the subsidiary company of which the customer trades with*;

2.3 In all material instances, the consent of the customer is obtained based on the fact that the Group makes the customer aware of **what** information is required to be collected and processed, **why** it is collected, **how** it will be collected and processed, **where** it will be processed and **to whom** that information will be given to.

2.4 The starting point with regards to the collection of personal information of a customer lies in the Group Companies respective Standard Terms and Conditions in respect of which the Customer provides consent for the use of its information to assess the creditworthiness of the Customer by the Group Company when it fills in and signs the Credit Application Form. By signing the Credit Application Form, and subject to no deletions in this regard, the Customer is deemed to have provided its consent;

2.5 In some cases, a Customer refuses to accept the Group Companies Standard Terms and Conditions and will insist that their terms and conditions of trade with Suppliers is signed instead. Such terms and conditions are, as per the Contract Management Policy of the Group, required to be sent to Group Legal for assessment. If such terms and conditions do not provide similar consents, it shall still remain the policy of the Group to abide by the provisions of the Act by collecting and processing information in the manner as contemplated in 2.2 above.

3. PARAMETERS OF DISCLOSURE OF PERSONAL INFORMATION

3.1 A customer's personal information may be disclosed from a Group Company to another Group Company for the purposes of providing the customer with the opportunity to engage with the Group's range of products housed in the respective Group Companies. However, personal information relating to a customer for trade with more than one Group Company shall follow the same procedure in the collection and processing of the customer personal information as contemplated in 2.2 above;

3.2 A customer's personal information may also be disclosed to third parties where the Group Company whom it trades with or the Group is required to do so in terms of applicable legislation, the law or where deemed necessary to protect the rights of the Group Company or the Group;

3.3 In terms of 3.1 and 3.2, the Group Finance Department is responsible for the collection and processing of Customer information regarding the activation of the Customer from an incidental credit perspective. With particular reference to 3.2, if it is necessary for the personal information of the Customer to be disclosed to third parties (read CGIC, Enviro Check or a credit bureau, this would be in accordance with the provisions of: (i)assessing the creditworthiness of the Customer and (ii) conducting due diligences on the customer with reference to complying with the Group's policies relating to fraud, crime, money laundering, anti-trust, anti-bribery and corruption and sanction listed companies internationally;

3.4 In terms of 3.3, it is contemplated that providing the Customer information to such third parties, would also be a necessary requirement for pursuing the legitimate interests of the Group provided that such service providers themselves have a duty of responsibility to collect and process such information for the specific purpose required.

4. AMENDMENTS TO PERSONAL INFORMATION

4.1 Customers have the right, at all material times, to access the information in the possession of a Group Company that it trades with and further the customer can ask for the updating, collecting or deletion of personal information on reasonable grounds. The deletion of personal information is subject to the Group not being restricted to comply thereto by means of prevailing legislation or to protect the legitimate interests of the Group;

4.2 The Group shall take all reasonable steps to confirm a customer's identity before providing details of their personal information or making changes to personal information.

5. SAFEGUARDING CUSTOMER INFORMATION

5.1 This condition imposed by POPI requires that the Group adequately protects the personal information of the customer and in this regard, key consideration will be given taking into account the following:

- the integrity and confidentiality of personal information in possession OR under the control by taking appropriate and reasonable measure to prevent the loss or damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information of the customer;
- have regard to generally and reasonably accepted information security practices and procedures;
- take reasonable steps to identify reasonable and foreseeable risks to personal information in the possession and control of the Group and establish and maintain safeguards against the risks identified and implement the safeguards, continually update them and regularly verify them.

5.2 With specific reference to the personal information obtained from a Customer by the Group Finance Department, access to the departments electronic files are restricted to designated Managers and employees who are required to process the data with permitted authorisation levels to access such data. Physical documents of Customer personal information is filed under lock and key and access to the Group Finance Department is restricted by third parties;

5.3 All the Group's electronic files/data are backed up daily and stored off site and safeguards are in place for the protections of such files and data which is administered by the Group IT department along strict protocols;

6. ACCESS TO DOCUMENTS

6.1 It is a mandatory requirement in the Group that the information belonging to the Group Companies and those of a customer must be dealt with in strict confidence and may only be disclosed where there is no fear of redress such as:

- disclosure is subject to a legal (statutory or regulatory) requirement;
- where there is a duty to the public to disclose such as where the public interest outweighs any interference with the privacy of the individual or customer or to prevent or mitigate a serious or imminent threat to public health;
- where the interests of the Group require disclosure;
- where the disclosure is made with the express or implied consent of the customer ;

6.2 DISCLOSURE TO THIRD PARTIES

6.2.1 All employees of the Group have a duty of confidentiality to the Group and have signed acknowledgment of such duty with the relevant Group Company in which they are employed. Accordingly, customer information may only be given to a third party if the customer has consented thereto in writing and the Group Company General Manager or Group Financial Officer has confirmed agreement thereto as well;

6.2.2 Confidential information or information belonging to a Group Company may not be disclosed to third parties without the consent of the General Manager, the Group Financial Officer and Group Legal;

7. STORAGE OF DOCUMENTS

7.1 The storage of hard copy documents, whether they are Group documents, customer information and supplier information may be required to be kept for periods as stipulated by prevailing legislation. Accordingly, the request by a customer to destroy personal information may not be complied with due to a prevailing statutory or regulatory requirement. In the event of uncertainty, contact Group Legal for clarity;

7.2 A few examples are:

- Companies Act – 7 Years and in some cases, indefinitely;
- Financial Intelligence Centre Act (FICA)- 5 years;
- Compensation for Occupational Injuries & Diseases Act (COIDA)- Vary from 40 years to 3 years;
- South Africa Revenue Services Acts- 5 years;

7.3 Electronic storage of information in the Group must be done in conjunction with Group IT and comply with the policies and procedures of Group IT;

7.4 The Electronic Communications Act 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 and 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. In this regard, IT is required to ensure that such "Business Information" is stored and archived in line with the Group's policy on the Control and Retention of Documents and Records.

7.5 Personal information that has become obsolete must be destroyed. Obsolescence does not require a consent to be destroyed other than confirmation thereof from the Chief Information Officer. Such obsolete information must be destroyed in a manner that it is not able to be reconstituted in a legible format.

7.6 The Group has a policy and procedure for the storage of and destruction of electronic data;

8. GROUP INFORMATION OFFICER

8.1 POPI prescribes the appointment of an Information Officer who is responsible for the compliance with the conditions of the lawful processing of personal information and compliance with the provisions of POPI.

8.2 The details of the Group Information Officer

are: Name: **Michelle Grobbelaar**

Email: michelle.grobbelaar@greencorp.co.za

Physical Address: Unit 7, Nordyk Park 5, Malmesbury Industrial 7300