GROOT CONSTANTIA TRUST NPC RF

PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

COMPLIANCE POLICIES
30 JUNE 2021

GESTIG 1685 FOUNDED

GROOT CONSTANTIA

LANDGOED • ESTATE

GROOT CONSTANTIA TRUST NPC RF

POPIA COMPLIANCE : POLICIES

CONTENT	PAGE NO.
Registration of Information Officer	1
Information Privacy Policy and Framework	2 - 8
Acceptable Usage Policy	9 - 13
Access Management Policy	14 - 17
Information Quality Policy	18 - 20
Backup and Restoration Policy	21 - 25
Information Security Policy	26 - 28
Physical and Environmental Security Policy	29 - 32
Bring Your Own Device Policy	33 - 36
Information Transfer Policy	37 - 40
Clean Desk and Clear Screen Policy	41 - 43
Retention and Destruction Policy	44 - 49
Website Privacy Policy	50 - 52
Handling and Processing of Requests Policy	53 - 56
Information Incident Management Policy	57 – 61

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

REGISTRATION CERTIFICATE

Registration Number:665/2021-2022/IRRTT

This is to certify that **Jean Naude** has been registered with the Information Regulator by **Groot Constantia Trust NPC RF** as the Information Officer in terms of section 55(2) of the Protection of Personal Information Act 4 of 2013 with effect from **18 May 2021**.

Chief Executive Officer
INFORMATION REGULATOR

NB: *Please note that it is your responsibility to ensure that the particulars of an Information Officer and/or Deputy Information Officer(s) are correct and updated on an annual basis or as and when it becomes necessary.*

Information Privacy Policy and Framework (POPIA and GDPR)

1. SCHEDULE
2. POLICY STATEMENT
3. DEFINITIONS OF TERMS USED IN THIS POLICY
4. PURPOSE AND SCOPE OF THE POLICY
5. PRIVACY COMPLIANCE FRAMEWORK
6. INFORMATION GOVERNANCE
7. INFORMATION PROCESSING PRINCIPLES
8. REVIEW OF POLICY

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF
1.2	Registration number : 1993/003391/08
1.3	VAT registration number : 4030108080
1.4	Physical address
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806
1.5	Email address : ceo@grootconstantia.co.za

2. POLICY STATEMENT

2.1. Every person has rights with regard to how their personal information is handled and protected. In order to carry out its business and provide its services, the company set out in item 1 of the Schedule (**"Company"**) may collect, store and process personal information about:

2.1.1. employees;
2.1.2. customers;
2.1.3. consumers;
2.1.4. service providers / suppliers; and
2.1.5. business contacts.

2.2. The Company recognises the need to treat this information in an appropriate and lawful manner. The Company is committed to complying with its obligations in this regard in respect of all personal information it handles, in a manner which maintains the confidence of the Company's customers, service providers / suppliers, business contacts and employees.

2.3. The Protection of Personal Information Act no. 4 of 2013 (**"POPIA"**) and regulations (2018) relate to identifiable, living, natural persons and identifiable, existing, juristic persons. The European Union General Data Protection Regulation (**"GDPR"**) only relates to the information of European Citizens (natural persons). Additional privacy legislation may also be applicable should the Company also conduct business in another country.

2.4. The types of information that the Company may be required to handle include details of current, past and prospective employees, service providers / suppliers, customers, consumers and other business contacts that the Company communicates with. The information would typically include names, addresses, email addresses, dates of birth, identity / passport numbers, phone numbers, private and confidential information and, potentially, special personal information. In addition, the Company may occasionally be required to collect and use certain additional types of personal information to comply with the requirements of the law.

2.5. The information may be stored on paper, electronically or by other media and is subject to certain legal safeguards specified in POPIA and GDPR, and potentially other applicable acts and regulations. The provisions of POPIA and GDPR impose restrictions on how the Company may collect and process the personal information in question.

2.6. This information privacy policy ("**Policy**") may be amended from time to time. Any breach of this Policy will be taken seriously by the Company and may result in disciplinary action being taken, which could include dismissal.

3. DEFINITIONS OF TERMS USED IN THIS POLICY

3.1. **POPIA Definitions**

3.1.1. **"data subject"** means all living, identifiable natural or juristic persons about whom the Company holds personal information or special personal information;

3.1.2. **"operator"** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

3.1.3. **"personal information"** means information relating to an identifiable, living, natural or juristic person, including (i) factual information, such as identity and passport numbers, names, addresses, phone numbers, email addresses and the like, or (ii) opinions regarding a data subject, such as a performance appraisal;

3.1.4. **"processing POPIA"** means any operation or activity, whether or not by automatic means, concerning personal information, including the:

3.1.4.1. collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information;

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

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

3.1.5. **"responsible party"** means a public or private body, or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information; and

3.1.6. **"special personal information"** means more sensitive information about an individual that pertains to racial or ethnic origins, political, religious or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a data subject of an offence or any proceedings in respect of any offence allegedly committed by a data subject, which can only be processed under strict conditions and will usually require the express written consent of the data subject concerned.

3.2. **GDPR Definitions**

3.2.1. **"controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

3.2.2. **"personal data"** means any information relating to an identified or identifiable natural person ("**data subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and

3.2.3. **"processing GDPR"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and

3.2.4. **"processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

4. PURPOSE AND SCOPE OF THE POLICY

4.1. This Policy sets out the Company's general rules and the important legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of identifiable personal and special personal information.

4.2. This Policy also describes the privacy compliance framework and information governance of the Company in detail.

4.3. This Policy is applicable to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**").

5. PRIVACY COMPLIANCE FRAMEWORK

5.1. **BACKGROUND**

5.1.1. To ensure compliance with the requirements of relevant privacy legislation such as POPIA and GDPR, the focus areas that must be addressed to be compliant are as follows:

5.1.1.1. governance;

5.1.1.2. people;

5.1.1.3. process; and

5.1.1.4. technology.

5.2. **PRIVACY COMPLIANCE FRAMEWORK**

5.2.1. **Focus on governance**

5.2.1.1. The Company undertakes to take accountability for its actions by implementing good corporate governance.

5.2.1.2. The focus on governance means that the Company will establish an Information Governance Committee ("**IGC**") and other structures to ensure that data protection compliance is an ongoing process and that continued management of information processes takes place.

5.2.2. **Focus on process**

5.2.2.1. The Company undertakes to implement processes to ensure that personal information is processed in line with relevant legislation.

5.2.2.2. This will include performing a Personal Information Impact Assessment ("**PIIA**"), as required by regulations promulgated under POPIA, and also developing and implementing the necessary policies and procedures and other control measures to ensure compliance with the relevant privacy legislation.

5.2.3. **Focus on people**

5.2.3.1. Most information security breaches involve people in one way or another. The Company undertakes to ensure that Users are made aware of their responsibilities in relation to processing personal information.

5.2.3.2. Users must undergo privacy and information security training at least annually and all new employees must be appropriately trained within 3 (Three) months of commencing employment with the Company.

5.2.4. **Focus on technology**

5.2.4.1. The Company undertakes to implement technology with appropriate security safeguards. The reference to "technology" includes software, hardware and data specific requirements. Appropriate security technological safeguards must be in place where personal information is processed, stored and destroyed. The Company undertakes to appoint a specialist in information technology ("**IT**") to set up and manage the Company's technology. This will be done either by in-house employees or by outsourcing this IT function to a compliant third party.

5.2.5. **Review and audit**

5.2.5.1. **Review and continuous monitoring**: The Company will ensure that the following is reviewed and monitored on an ongoing basis:

5.2.5.1.1. That the Company's Governance Processes are functioning as intended and that regular IGC's have been established;

5.2.5.1.2. That the Company's processes have been reviewed on a regular basis and that all policies and procedures have been reviewed and updated at least annually;
5.2.5.1.3. That the Company's other control measures that have been implemented are functioning as intended and that they are adequate and effective;
5.2.5.1.4. That the Company's management and employees have been made aware and kept aware of how to process personal information and that a privacy awareness campaign has been developed and implemented;
5.2.5.1.5. That the Company's safety and security technology areas have undergone annual vulnerability assessments and, where applicable, that penetration testing has been done. This also includes information security management.

5.2.5.2. **Identify the gaps**

5.2.5.2.1. On a regular basis, gaps or weaknesses ("**Gap/s**") should be identified and actions to mitigate such Gaps should be recorded in a Privacy Implementation Action Plan ("**PIAP**").
5.2.5.2.2. The Gaps should be prioritised and an accountable person should be appointed to rectify the Gaps.
5.2.5.2.3. A due date should be set by when the Gaps should be rectified.

5.2.5.3. **Action the gaps**

5.2.5.3.1. The Gaps should be actioned in accordance with the PIAP.
5.2.5.3.2. A specific responsible person should be identified to co-coordinate or perform an action and a due date to complete the action in question should also be set.
5.2.5.3.3. Where there is a specific due date set, the progress to address the Gaps should be reported to the IGC.

5.2.5.4. **Audit the implementation**

5.2.5.4.1. The Company undertakes to review the efficacy of the controls implemented to address and rectify the Gaps that have been identified.
5.2.5.4.2. The Company undertakes to ensure that the abovementioned review is conducted by an independent party not involved in the initial implementation. Where it is not possible to appoint an independent party within the Company then the review may be outsourced to independent third party auditors.

5.2.5.5. **Assess the outcome**

5.2.5.5.1. The Company undertakes to assess the outcome of the audit and determine what action must be taken, if any, to address the Gaps. Where the Gap has been addressed and rectified, it must be noted. Where there is additional work required to be done, it must be added to the PIAP.

5.2.5.6. **Continuous reporting**

5.2.5.6.1. The Company undertakes to continuously report the status of the management of personal information to the IGC and, at least on a quarterly basis, to the board of directors of the Company.

6. INFORMATION GOVERNANCE

6.1. INFORMATION OFFICER

6.1.1. The responsibilities of the information officer designated in terms of the POPIA include:
6.1.1.1. the encouragement of compliance, such as awareness and training, by the Company, taking into consideration all of the conditions for the lawful processing of personal information;
6.1.1.2. ensuring compliance by the Company with the provisions of POPIA;
6.1.1.3. dealing with requests made to the Company in terms of POPIA, such as requests made from data subjects to update or view their personal information;
6.1.1.4. working with the information regulator ("**Regulator**") in relation to investigations; and
6.1.1.5. the designation and delegation of relevant duties to deputy information officers appointed by the Company.

6.1.2. The responsibilities of the information officer have been expanded upon in the regulations promulgated under POPIA on 14 December 2018. In this regard, the information officer must ensure that:
6.1.2.1. a compliance framework is developed, implemented, monitored and maintained;
6.1.2.2. a PIIA is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
6.1.2.3. a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000;
6.1.2.4. internal measures are developed, together with adequate systems, to process requests for information or access thereto; and
6.1.2.5. internal awareness sessions are conducted regarding (i) the provisions of POPIA, (ii) regulations promulgated in terms of POPIA, (iii) relevant industry codes of conduct, or (iv) information obtained from the Regulator.

6.2. INFORMATION GOVERNANCE COMMITTEE RESPONSIBILITES

6.2.1. **Strategic**: The oversight of the full information lifecycle for both structured and unstructured information, including:
6.2.1.1. endorsement of information policies, principles and procedures in relation to information management;
6.2.1.2. assisting with ensuring compliance with the provisions of POPIA and GDPR, where applicable, which include the following:
6.2.1.2.1. The security and integrity of data/information held by, or on behalf of ,the Company;
6.2.1.2.2. The dissemination of the Company's data/information to third parties;
6.2.1.2.3. Information and data confidentiality and availability;
6.2.1.2.4. Information and data quality, including completeness, accuracy and ensuring that information is up to date;
6.2.1.2.5. Information sharing arrangements with other parties;
6.2.1.2.6. Retention and destruction of information practices;
6.2.1.2.7. Document management, including the digitisation of documents; and
6.2.1.2.8. Discussing and identifying the areas where consent will be needed for the processing of personal information.
6.2.1.3. assisting with the integration of people, technologies, information and processes across the Company;
6.2.1.4. identifying and assessing the information risks and provide input to the Company's enterprise wide risk management process;

6.2.1.5. ensuring that there is proactive monitoring of data/information breach incidents and review the response to these incidents;
6.2.1.6. reviewing and provide oversight to ensure that the information architecture supports confidentiality, integrity and availability of information;
6.2.1.7. endorsing information-related strategies and roadmaps;
6.2.1.8. prioritising information-related initiatives;
6.2.1.9. establishing information-related metrics and oversight of results;
6.2.1.10. directing efforts to resolve issues in relation to information management;
6.2.1.11. assisting with advice on the leverage of information to sustain and enhance the Company's intellectual capital; and
6.2.1.12. reviewing and assessing the actions taken to monitor the effectiveness of information management and how the outcomes were addressed.

6.2.2. **Operational**: The IGC will:

6.2.2.1. establish structures needed to support information governance in the Company;
6.2.2.2. delegate authorities for the implementation of decisions;
6.2.2.3. co-ordinate information management responsibilities across the Company to ensure complete coverage of the information lifecycle;
6.2.2.4. make the Users aware of the IGC and its roles and responsibilities;
6.2.2.5. promote good information management practices and publish the names of the Information Asset Owners ("**IAO's**") for easy reference so they can be notified of particular issues relating to their domain; and
6.2.2.6. train and mentor IAOs to enable them to fulfil their roles.

7. INFORMATION PROCESSING PRINCIPLES

7.1. **POPIA**: The Company fully supports and complies with the 8 (Eight) protection principles of POPIA which are summarised below:

7.1.1. **Accountability**: a responsible party must ensure that the information processing principles are complied with;
7.1.2. **Processing limitation**: personal information must be processed lawfully and in a reasonable manner;
7.1.3. **Purpose specification**: personal information must be obtained/processed for specific lawful purposes;
7.1.4. **Further processing limitation**: further processing of personal information must be in accordance or compatible with the purpose/s for which it was originally collected;
7.1.5. **Information quality**: personal information must be complete, accurate, not misleading and kept up to date;
7.1.6. **Openness**: personal information may only be processed by a responsible party who has taken reasonable steps to notify the data subject;
7.1.7. **Security safeguards**: personal information must be kept secure, and its confidentiality and integrity must be maintained; and
7.1.8. **Data subject participation**: a data subject has the right to request the responsible party to confirm, free of charge, whether or not the responsible party holds personal information, together with a description of the personal information held by such responsible party.

7.2. **ACCOUNTABILITY**

7.2.1. The provisions of POPIA are intended not to prevent the processing of personal information, but to make sure that a responsible party ensures that the information processing principles as set out in POPIA, and all the measures that give effect to the principles, are complied with.
7.2.2. The data subject must be told the identity of the responsible party (in this case, the Company) and the purpose for which personal information is to be processed by the Company.
7.2.3. This Policy, developed by the Company to protect privacy, is available at the Company premises and is also accessible online at the Company's website. This Policy outlines the Company's commitment to privacy.

7.3. **PROCESSING LIMITATION**

7.3.1. For personal information to be processed lawfully, certain conditions have to be met. These may include, amongst other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. When special personal information is being processed, in most cases the data subject's explicit consent to the processing of such special personal information will be required.
7.3.2. A responsible party must collect personal information directly from the data subject unless (i) information is in a public record, (ii) the data subject has consented, (iii) the collection of personal information does not prejudice the legitimate interest of the data subject, or (iv) collection is necessary to comply with, or to avoid prejudice with or to the maintenance of, laws; to enforce legislation concerning the collection of revenue; for purposes of proceedings in a court; or in the interest of national security.
7.3.3. Where the Company processes personal information as a responsible party, the data subject should be informed of this fact. The data subject should also be informed for what purpose the personal information is being processed by the Company, and where or to whom such personal information may be disclosed or transferred. The Company has drafted a "Terms of Use" document which can be found online at the Company's website, which explicitly outlines how and in what circumstances the Company may use a person's information.

7.4. **PURPOSE SPECIFICATION**

7.4.1. Personal information may only be processed for a specific and lawful purpose, or for any other purpose specifically permitted by POPIA, and steps must be taken to ensure that the data subject is aware of the purpose of the collection of the personal information. The Company undertakes not to (i)collect personal information for one purpose and then use the personal information for another purpose, or (ii) retain personal information for any longer than is necessary for achieving the purpose for which the information was collected.
7.4.2. Personal information should only be collected to the extent that it is required for the specific purpose communicated to the data subject. Any personal information which is not necessary for that purpose should and will not be collected by the Company.
7.4.3. If it becomes necessary to change the purpose for which the personal information is processed, the data subject will be informed of the new purpose before any processing occurs. Any employee personal information collected by the Company will be used for ordinary human resources purposes. Where there is a need to collect employee personal information for any other purpose, the

Company will notify the employee in question of this and, where it is appropriate and practicable, the Company will get the employee's consent prior to such processing.

7.4.4. Where the Company collects personal information directly from a data subject, the personal information collected and processed by the Company, such as identity number, proof of address and the like, will only be used for the required purpose.

7.5. **FURTHER PROCESING LIMITATION**

7.5.1. Personal information should not be kept longer than is necessary for the purpose for which it was collected. For guidance in relation to a particular personal information retention period, a User should contact the Company. The Company has various legal obligations to keep certain personal information of Users for a specified period of time. In addition, the Company may need to retain personal information for a period of time to protect its legitimate commercial and other interests.

7.5.2. The Company will not use any personal information for any purpose other than that for which it received the information in the first place, unless any further processing of such information is compatible with the original purposes for which the information was collected.

7.6. **INFORMATION QUALITY**

7.6.1. Personal information must be complete, accurate, and kept up to date. Personal information which is incorrect or misleading is not accurate and steps will be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal information will be destroyed. Employees should ensure that they notify their manager / human resources of any relevant changes to their personal information so that it can be updated and maintained accurately.

7.6.2. All personal information which is in paper form should be destroyed only by shredding. If the personal information is held electronically, the Company must ensure that a reputable service provider destroys the personal information so that there is no future record of the information and the Company must obtain an undertaking from the applicable service provider in this regard.

7.7. **OPENNESS**

7.7.1. Personal information may only be processed by the Company if the Company has notified the data subject that the Company has obtained the information from legitimate sources.

7.7.2. In cases where the Company works directly with a data subject, the Company will take reasonable, practicable steps to ensure that the data subject is aware of the following:

7.7.2.1. What information is being collected and, where it is not collected from the data subject, the source of the information;

7.7.2.2. The full name and addresses of the Company;

7.7.2.3. The purpose for which the information is being collected;

7.7.2.4. Whether supplying the personal information to the Company is voluntary or mandatory;

7.7.2.5. The consequences of failure to provide the information;

7.7.2.6. The applicable law authorising or requiring the collection of the information;

7.7.2.7. The right to lodge a complaint against the Company the Regulator; and

7.7.2.8. Any further relevant information, such as recipient or category of recipients of information, nature of information, existence of the right of access and the right to rectify information collection.

7.8. **SECURITY SAFEGUARDS**

7.8.1. The Company and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information.

7.8.2. The Company will put in place procedures and technologies to maintain the security of all personal information. Personal Information may only be transferred to an operator if the operator has agreed to comply with those procedures and policies or has adequate security measures in place.

7.8.3. Users may refer to the Company's information security and related policies for further information concerning the Company's security safeguards.

7.8.4. The following principles must be maintained by the Company:

7.8.4.1. **Confidentiality**: that only people who are authorised to use the personal information in question can access it. The Company will ensure that only authorised persons have access to an employee's personnel file and any other personal or special information held by the Company. Employees are required to maintain the confidentiality of any personal information and / or special personal information that they have access to.

7.8.4.2. **Integrity**: that proper security safeguards are in place to ensure the maintenance and assurance, of the accuracy and consistency of information / data over its entire life cycle.

7.8.4.3. **Availability**: that authorised users should be able to access the personal information if they need it for an authorised purpose.

7.8.5. Examples of security procedures at the Company include:

7.8.5.1. Secure lockable desks and Cupboards – desks and cupboards must be kept locked if they hold confidential personal identifiable information of any kind;

7.8.5.2. Methods of Disposal – paper documents must be shredded. CD-ROMs and USB keys should be physically destroyed when they are no longer required;

7.8.5.3. Equipment – data users must ensure that individual computer monitors do not show confidential information to passers-by and that they log off from their computer when it is left unattended; and

7.8.5.4. User Management – any access to the Company database is logged by the Company through a username and password system. Any changes / updates / uploads to the system are constantly tracked.

7.8.6. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Company or any third party processing personal information under the authority of the Company, must notify the Regulator and the data subject as soon as is reasonably possible, taking into consideration the time that is taken by the Company to determine the scope of the breach and to restore the integrity of its information systems.

7.8.7. Any notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

7.8.7.1. Mailed to the data subjects last known physical or postal address;

7.8.7.2. Sent by email to the data subjects last known email address;

7.8.7.3. Placed in a prominent position on the website of the Company;

7.8.7.4. Published in the news media; or
7.8.7.5. As directed by the Regulator.

7.8.8. The notification referred to above must provide sufficient information to all the affected data subjects to take protective measures against the potential consequences of the security compromise including:
7.8.8.1. a description of the possible consequences of the security compromise;
7.8.8.2. a description of the measures that the Company intends to take or has taken to address the security compromise;
7.8.8.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
7.8.8.4. if known to the Company, the identity of the unauthorised person who may have accessed or acquired the personal information in question.

7.9. **DATA SUBJECT PARTICIPATION**

7.9.1. A formal request from a data subject for information that the Company holds about them must be made in writing, accompanied with adequate proof of identification (in most instances, a certified copy of the individual's identity document or passport and proof of residence will be sufficient).

7.9.2. Any employees who receive a written request in respect of data held by the Company must forward it to the information officer immediately.

7.9.3. Any individual requesting personal information that may be held by the Company will be referred by the relevant employee to whom the request was made to the information officer, who will process the request. The information officer will either process the request directly, or will direct such employee to request a certified copy of the individual's identity document or passport as well as proof of address. Once this is received, the employee will then be authorised to release the personal information to the individual. The employee must:
7.9.3.1. record the request in the request register / system; and
7.9.3.2. safely store the certified copy of the identity document and passport either in a file in a locked cupboard (if in paper format) or online in an encrypted folder which cannot be accessed by unauthorised personnel. Storage of these documents should be kept for 1 (one) year, after which they must be properly destroyed.

7.9.4. Any employee dealing with telephonic enquiries from data subjects should guard against disclosing any personal information held by the Company over the phone. In particular, the employee must:
7.9.4.1. check the identity of the caller to ensure that information will only be given to a person who is entitled to that information – this can be accomplished by confirming: identity number, date of birth, address, cell phone number and the like;
7.9.4.2. request that the caller put their request in writing if the employee is not completely sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified. In these circumstances, the employee should also request that a certified copy of the identity document / passport of the individual is provided before information is released;
7.9.4.3. refer the request to their manager for assistance in difficult situations. No employee should feel forced to disclose personal information; and
7.9.4.4. where a request has been made in terms of this section, and personal information is communicated to the data subject, the data subject must be advised of their right to request the correction of the information.

7.9.5. The data subject may request that the Company correct or delete personal information which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or to destroy such record of personal information. If such a request is made, the Company must send this request to the appropriate party within the Company who should then correct the information, destroy or delete it, and provide the data subject with credible evidence that this has been done.

7.10. **GDPR**

7.10.1. The Company fully supports and complies with the 6 (Six) protection principles of the GDPR which are summarised below:
7.10.1.1. **Lawfulness, fairness and transparency**: The personal information of the European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
7.10.1.2. **Purpose limitation:** The personal information of the European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.
7.10.1.3. **Data Minimisation**: The personal information of the European citizens will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
7.10.1.4. **Accuracy**: The personal information of the European citizens will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.
7.10.1.5. **Storage Limitation**: The personal information of the European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
7.10.1.6. **Integrity and Confidentiality**: The personal information of the European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. REVIEW OF POLICY

The Company will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, taking into account changes in the law and organisational or security changes.

Acceptable Usage Policy

1. SCHEDULE
2. PURPOSE
3. SCOPE
4. POLICY
5. USAGE GUIDELINES
6. RIGHTS RESERVED BY THE COMPANY
7. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
8. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF
1.2	Registration number : 1993/003391/08
1.3	VAT registration number : 4030108080
1.4	Physical address
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806
1.5	Email address : ceo@grootconstantia.co.za

2. PURPOSE

This acceptable usage policy ("**Policy**") clearly indicates what information employees, contractors, visitors, or other persons authorised to access and use the Company's systems ("**Users**") are and are not permitted to use. It is important to apply information security principles to protect the confidentiality, integrity and availability of information. The potential exists that, without this Policy, Users could violate information security and avoid punitive actions by claiming not to be aware about any restrictions that the company set out in a 1.1 of the Schedule ("**Company**") has in place.

3. SCOPE

This Policy applies to all Users of any and all information systems that belong to the Company.

4. POLICY

4.1. The Company will issue various acceptable usage guidelines in this Policy covering the following items:
- 4.1.1. Computer and information technology ("**IT**") system usage;
- 4.1.2. Software and data usage;
- 4.1.3. Internet and email usage;
- 4.1.4. Newsgroups;
- 4.1.5. Telephone usage;
- 4.1.6. Office equipment and materials usage;
- 4.1.7. Social media usage;
- 4.1.8. Video conferencing;
- 4.1.9. IT security; and
- 4.1.10. Privacy and confidentiality.

4.2. As a requirement of IT system access, and as a component of security awareness training, all Users, whether employees of the Company or third parties, will be required to provide signed acceptance of this Policy, confirming such User's acknowledgement that he / she is bound by all provisions set out in this Policy. A copy of the signed document will be provided to the User in question, and the original will be retained by the Company.

4.3. Compliance with the provisions of this Policy is a combined effort that requires Users to act responsibly and to guard against abuse. Each User has an obligation to abide by all standards of acceptable and ethical use as described in this Policy. Each User must:
- 4.3.1. protect the access and integrity of computing and IT resources;
- 4.3.2. abide by all applicable laws and respect the intellectual property rights of others, including the legal use of licensed software;
- 4.3.3. respect the privacy and personal rights of others; and
- 4.3.4. ensure that Company sensitive information must not be forwarded to any party outside the Company without prior approval from the chief executive officer ("**CEO**").

5. USAGE GUIDELINES

5.1. **Computer and IT system usage**
- 5.1.1. Systems, including computers and other related technology, are the property of the Company.
- 5.1.2. Access to, and use of, Company systems and their components will be monitored and controlled at all times.

5.1.3. Compliance with the usage guidelines set out in this Policy is a combined effort that requires Users to act responsibly and guard against abuse. Therefore, each User has an obligation to abide by the following standards of acceptable and ethical use as described in this Policy. The following conduct is not permitted:

5.1.3.1. Accessing computers, computer software, computer data or information, or networks without proper authorisation, regardless of whether the Company owns the computer, software, data, information, or network in question;

5.1.3.2. Transmitting on or through any of the Companies systems, services, or products any material that is unlawful, obscene, racial, pornographic, threatening, abusive, libellous, or hateful, or encourages conduct that may constitute a criminal offence, may give rise to civil or any other liability, or otherwise may violate any local, state, national or international law;

5.1.3.3. Consuming excessive resources, including central processing unit time, memory, disk space and the like, and all session time for personal use, is prohibited. The use of resources-intensive programs, which negatively affect other Users, or the performance of the Company's systems or networks is also not permitted; and

5.1.3.4. Intercepting or examining the content of messages or files in transit on a network without authorisation from the owner of the information, including when it is not specifically part of the function of the User to perform such an action.

5.2. **Software and data usage**

5.2.1. The software tools of the Company, and the data they create and process, belong to the Company.

5.2.2. Software is to be used for its intended purpose only. It is not to be copied, reverse-engineered, distributed, installed, and / or deleted without appropriate authorisation.

5.2.3. Data is to be used for its intended purpose. It is not to be copied, distributed, edited, appended, or deleted without appropriate authorisation.

5.2.4. Violating any software license agreement or intellectual property right, including copying, adapting or redistributing copyrighted software, data, or reports without proper, recorded authorisation, is prohibited.

5.2.5. Violating the intellectual property rights of software holders, or the holders of computer-generated data or reports, without proper, recorded authorisation, is prohibited.

5.3. **Internet and email usage**

5.3.1. Internet and email usage must be restricted, as both activities make use of public and unsecured networks.

5.3.2. The Internet is to be used for business purposes only and usage will always be monitored and controlled by the Company.

5.3.3. Email is to be used for business purposes only and usage will always be monitored and controlled by the Company.

5.3.4. Causing security breaches or disruptions of internet communications is strictly prohibited. Security breaches include, without limitation, (i) accessing data not intended for the User in question, or (ii) logging onto a server or account that the User is not expressly authorised to access.

5.3.5. When reference is made to, "disruption" in this clause 5, it shall include, without limitation, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, attempts to crash a host, and the introduction of any malicious code, such as computer viruses or "trojans", onto any part of the Company's computer network.

5.3.6. Usage specifically associated with email:

5.3.6.1. It is a violation of this Policy to send emails that contain personal identifiable information as described in the Protection of Personal Information Act 4 of 2013 ("POPIA"), without considering the appropriate protection required in relation to such emails. Emails of this nature must at the very least be password protected.

5.3.6.2. It is a violation of this Policy to send email that is abusive or threatens an individual's safety. The use of email for sexual, ethnic, religious, or any other harassment is also prohibited. Threats to personal safety should be reported to the Company immediately.

5.3.6.3. It is a violation of this Policy to use email to harass an individual. Sending or forwarding chain letters and / or deliberately flooding a User's mailbox with automatically generated mail that is designed to interfere with proper mail delivery or access is expressly prohibited.

5.3.6.4. Sending unsolicited email, including the sending of junk mail or other advertising material to individuals who did not specifically request such material is prohibited. Sending unsolicited bulk mail messages is expressly prohibited. If a recipient has asked to stop receiving email, the User may not send the recipient any further email. This does not apply to normal business information messages.

5.3.6.5. Creating or forwarding pyramid schemes of any type, whether or not the recipient wishes to receive such mailings is prohibited.

5.3.6.6. Malicious email including, without limitation, flooding a User or site with very large or numerous pieces of email is prohibited.

5.3.6.7. It is a violation of this Policy to forge an email signature to make it appear as though it originated from a different person, whether through unauthorised use, forging, mail header information alteration or any other method.

5.3.6.8. It is a violation of this Policy to use a company or a client account to collect replies to messages sent from another party.

5.3.6.9. It is a violation of this Policy to attempt to gain access to another person's email files, regardless of whether the access was successful or whether or not the messages accessed involved personal information, as this term is defined in POPIA.

5.3.6.10. It is a violation of this Policy to send unauthorised copyrighted materials electronically.

5.3.6.11. All Users are required to keep all login details, including username and passwords, confidential and may not share these details with any other person.

5.3.6.12. Users whose employment or other relationship with the Company has been terminated will have no rights of access to the contents of messages addressed to them, whether in an official or private capacity.

5.4. **Newsgroups**

5.4.1. The following serves as a guideline as to what the Company considers the misuse of computing resources and privileges. These actions are prohibited except when the User is authorised to do so by the Company as part of normal business practice and their specific function within, or in relation to, the Company:

5.4.1.1. Posting the same or similar messages to large numbers of newsgroups (known as newsgroup or USENET spam);

5.4.1.2. Posting encoded binary files to newsgroups not specifically named for that purpose;

5.4.1.3. Cancellation or superseding of posts other than a User's own posts, with the exception of official newsgroup moderators performing their duties;
5.4.1.4. Forging of header information, which includes the circumvention of the approval process for posting to a moderated newsgroup;
5.4.1.5. Solicitation of email from any other email address other than the User's account or service, with the intent to harass or collect replies; and
5.4.1.6. Posting of articles from the Company network or networks of other internet service providers on behalf of, or to advertise any service hosted by the Company or connecting via the Company's network without written permission from the Company.

5.5. **Telephone usage**

5.5.1. The telephone system, including all telephones and fax machines, is the property of the Company.
5.5.2. The telephone system, including all and analog and digital lines, is to be used for business purposes only and will be monitored and controlled by the Company at all times.

5.6. **Office equipment and materials usage**

5.6.1. All office materials, furnishings and supplies provided to Users are the property of the Company and are to be used for business purposes only.
5.6.2. Generic materials, such as pens, blank paper and the like, may be freely accessed but are not to be removed from the Company without the prior consent of the Company.
5.6.3. Specific materials such as letterheads must and will have restricted access and are not to be removed from the Company without the prior consent of the Company.
5.6.4. Users are not permitted to place any Company material, including software or internal memos, on any publicly accessible internal or external website without the prior approval of the CEO.

5.7. **Social Media usage**

5.7.1. The Company's social media accounts are intended to be used, and may only be used, solely for business purposes.
5.7.2. The following activities are deemed to be inappropriate use of social media:
5.7.2.1. Use of social media for illegal or unlawful purposes, including copyright infringement, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering including, without limitation, spreading of computer viruses;
5.7.2.2. Use of social media that in any way violates the Company's policies, rules, or administrative orders such as any code of conduct that may be applicable;
5.7.2.3. Opening attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with the utmost caution; and
5.7.2.4. Sharing social media account passwords with another person or attempting to obtain another person's social media account password.

5.8. **Video Conferencing**

5.8.1. Use of video conferring is for business purposes only and the following conditions must be adhered to:
5.8.1.1. Users are required to act professionally and respectfully at all times;
5.8.1.2. Video conferences are required to be treated like a normal meeting with a client;
5.8.1.3. No foul language should be used;
5.8.1.4. If a User's screen is being shared, such User is required to make sure that no Confidential data / Information of other clients or confidential Company data is displayed; and
5.8.1.5. Users are required to always use the highest security settings during all video conferences.

5.9. **IT Security**

5.9.1. A User must:
5.9.1.1. use only those computing and IT resources of the Company for which authorisation has been given;
5.9.1.2. use computing and IT resources of the Company only for their intended purpose;
5.9.1.3. always lock computers and mobile phone when not directly in use;
5.9.1.4. stay alert and always report any suspicious activity to the Company;
5.9.1.5. always password-protect sensitive files on computers, USB flash drives, smartphones or laptops;
5.9.1.6. always create complex passwords by including different letter cases, numbers, and punctuation. A User must also attempt to use different passwords for different websites and computers;
5.9.1.7. always ensure that, when plugging in personal devices such as USB's, MP3 players and smartphones, the device in question is not infected with a virus;
5.9.1.8. be cautious of suspicious emails and links. A User must always delete suspicious emails and never click on links or attachments; and
5.9.1.9. exercise caution when forwarding email or messages, as some information that is intended for a specific individual may not be appropriate for general distribution.

5.9.2. A User must not:
5.9.2.1. be tricked into giving away confidential information by responding to emails or calls requesting confidential information or personal information;
5.9.2.2. use an unprotected computer to access the Company's systems;
5.9.2.3. leave confidential or personal information in view of any person that should not have access to such information;
5.9.2.4. install unauthorised programs on any work computer;
5.9.2.5. furnish false data on any sign-up form, employment contract, or online application;
5.9.2.6. at any time misrepresent his / her identity, use an anonymous identity or someone else's identity, password or identity number, or address;

5.9.2.7. attempt to circumvent the user authentication or security of any host, network, or account. This includes, without limitation, accessing data not intended for the User, logging into a server or account that the User is not expressly authorised to access, or probing the security of other networks;

5.9.2.8. seek loopholes in computer security systems or attempt to gain knowledge of any password, or any other information used for authentication purposes. This may also not be done to attempt to damage computer systems, obtain extra resources, take resources from another User, gain access to systems or use systems for which proper authorisation was not given;

5.9.2.9. use any program / script / command, or send messages of any kind, designed to interfere with another User's session; and

5.9.2.10. execute any form of network monitoring which may intercept data not intended for a specific User's use.

5.10. **Privacy and confidentiality**

5.10.1. The following will be deemed to be a breach of privacy and confidentially:

5.10.1.1. Transmission, distribution, processing or storage of any information, data or material in violation of POPIA or any other applicable privacy laws or regulations;

5.10.1.2. a violation or infringement of any intellectual property right of any nature whatsoever; and

5.10.1.3. a contravention of the privacy rights of any natural person or juristic person under POPIA or any other applicable privacy laws or regulations.

6. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

7. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

8. POLICY AWARENESS AND UPDATE

8.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

8.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

8.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Access Management Control Policy and Procedure

1. SCHEDULE
2. INTRODUCTION
3. OBJECTIVE
4. SCOPE
5. DOCUMENTS
6. POLICY
7. PROCEDURE REGARDING ACCESS CONTROL
8. RIGHTS RESERVED BY THE COMPANY
9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
10. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. The company set out in item 1 of the Schedule ("Company") is committed to, and is responsible for, ensuring the confidentiality, integrity and availability of the data and information stored on its systems.

2.2. Access management to information and information processing facilities are important aspects to consider in order to ensure the confidentiality, integrity and availability of the information of the Company.

2.3. When capitalized terms are used in the policy and procedure document ("**Policy"**), they are given the meanings ascribed to them either (i) in the Policy itself, or (ii) in the Protection of Personal Information Act 4 of 2013 ("**POPIA"**).

2.4. The provisions set out in this Policy ensure that the Company complies with its obligations under POPIA insofar as the security of information regulated and protected by POPIA is concerned.

3. OBJECTIVE

3.1. The objective of this Policy is to formalise the access control management process for the Company. When reference is made to "access control" in this Policy, it effectively means that access to the Company's information and information processing facilities is limited through access control measures, such as usernames and passwords. Access control will be further enhanced by two factor authentication such as one-time pins where deemed necessary.

3.2. This Policy sets out the processes to be followed by the Company to:

3.2.1. limit the access to information and information processing facilities;

3.2.2. ensure authorised user access and to prevent unauthorised access to the Company's systems and services;

3.2.3. make employees, contractors, visitors, or other persons authorised to access and use the Company's systems (**"Users"**) accountable for safeguarding their authentication information; and

3.2.4. prevent unauthorised access to the Company's systems and applications.

3.3. Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important and valuable asset of the Company which must be managed with care at all times. All information has a value to the Company. However, not all of this information has an equal value, or requires the same level of protection. The Company will determine in its sole discretion which information requires a greater degree of protection, depending on the:

3.3.1. nature of the information in question; and

3.3.2. the Company's obligations in relation to such information, as regulated by the provisions of POPIA.

3.4. Access controls are put in place to protect information by:

3.4.1. controlling who has the right to use different information resources; and

3.4.2. guarding against unauthorised use of information.

3.5. Formal procedures must be followed to control how access to information is granted, changed and revoked.

4. SCOPE

4.1. This Policy is applied to all Users that use devices that relate to the Company's business operations where data is processed.

4.2. This Policy covers all servers, workstations, network devices, operating systems, applications and other information assets of the Company.

5. DOCUMENTS

5.1. This Policy should be read in conjunction with the following related policies and procedures of the Company:
- 5.1.1. Information Security Policy;
- 5.1.2. Acceptable Use Policy; and
- 5.1.3. Clean Desk and Clear Screen Policy.

6. POLICY

6.1. The Company understands the importance of protecting its information and information processing facilities from unauthorised access.

6.2. Access to information and information processing facilities are provided by the information asset owners, as identified in the information asset register. The information asset register (**"IAR"**) is an inventory of information assets that include information, software and hardware of the Company. The IAR also allocates information asset owners (**"IAO/s"**) to the specific assets set out in the IAR. The IAO's have a responsibility to only provide access to people where their role requires them to have access to the specific information or information asset. In smaller organisations it could be the chief operating officer ("**CEO"**) that provides access to information assets.

7. PROCEDURE REGARDING ACCESS CONTROL

7.1. **User Access Management**
- 7.1.1. User registration will only occur where the User's role within or in relation to the Company requires them to have access to the information or information processing facilities in question.
- 7.1.2. The User must complete the system access request form in order to gain access to the information or information processing facilities in question.
- 7.1.3. The access request by the User will be considered by the IAO and will be approved or declined by the IAO based on the need to obtain access to the information in question.
- 7.1.4. The Company has designated some Users as "privileged Users", and such Users will have access to root and administration functions. In such cases, the IAO may either decline or recommend access, but if access is recommended, the CEO of the Company will make the final decision as to whether access of the User in question is approved or declined.
- 7.1.5. Where the User activation has been approved in terms of this Policy, the relevant activation will be done within 48 (Forty-Eight) hours.

7.2. **Passwords**
- 7.2.1. Where username and passwords are used by the Company to manage access control to information or information processing facilities, the following factors and criteria must be applied:
  - 7.2.1.1. Passwords must be at least 8 (Eight) characters long and should include capital letters, lower case letters, numbers and special characters;
  - 7.2.1.2. Passwords should expire every 30 (Thirty) days, or if there is a onetime pin (second factor authentication) that is combined with the password, the expiry of passwords can be extended to 90 (Ninety) days;
  - 7.2.1.3. An incorrect password must be revoked after 3 (Three) incorrect passwords have been entered, and the system should indicate that the administrator be contacted to reset the password;
  - 7.2.1.4. When a new generic password has been provided, the password must be changed to a unique password by the User and cannot be used going forward;
  - 7.2.1.5. The User should not be able to use any of the past 10 (Ten) passwords that have been used previously;
  - 7.2.1.6. The password rules must be applied for both Users and privileged Users;
  - 7.2.1.7. There must be a "time-out" applied after a User has started a session and there has been no activity for a period of 10 (Ten) minutes ; and
  - 7.2.1.8. Passwords must be encrypted with at least a AES-128-bit or higher encryption standard.

7.3. **User Responsibilities**
- 7.3.1. Users are responsible for ensuring that they gain access to the Company's information and information processing facilities only for work that is in line with their role within, or in relation to, the Company. Users must do the following at all times:
  - 7.3.1.1. Protect their username and password and never share them with anyone else;
  - 7.3.1.2. Ensure that they log out of any Company system when they are not using the system in question;
  - 7.3.1.3. Comply with the Company's Acceptable Use policy, and all other policies and procedures of the Company that regulate the processing of information in terms of POPIA; and
  - 7.3.1.4. Make sure that their screen is cleared and use the lock function when they are not at their desks.

7.4. **User Deactivation**
- 7.4.1. Deactivation of a User's access will take place in the following circumstances:
  - 7.4.1.1. When the User is an employee and has resigned from the Company;
  - 7.4.1.2. When the User has been authorised to assist on a Company project and the project in question has been finalised; and
  - 7.4.1.3. Where the User is an employee has been suspended from the Company due to a forensic investigation.
- 7.4.2. Deactivation of access will take place as soon as possible, but not longer than 24 (Twenty-Four) hours from the time that a decision has been made by the Company to deactivate a User.

7.5. **Access Reviews and Reconciliation**
- 7.5.1. Periodic auditing of the accounts of Users will be performed by the IAO in order to:
  - 7.5.1.1. identify and revoke non-active, unused or non-authorised Users; or
  - 7.5.1.2. perform the reallocation or revocation of the privileges of Users.
- 7.5.2. Access reviews will take place as often as necessary, but will occur at least once every month.

7.6. **Privilege Management**

7.6.1. Assignment of account privileges of Users is based on the principal of minimum privilege. Thus, an authorised User will be provided with access sufficient for their role at, or in relation to, the Company and the User in question will not be afforded any greater level of access than that strictly required.

7.6.2. If an authorised User's role within, or in relation to, the Company changes at any time, such User's access rights to information and / or information processing facilities may also change to reflect the circumstances and requirements of their new role.

7.7. **Network Access Control**

7.7.1. The use of modems on the Company-owned personal computers connected to the Company's network can seriously compromise the security of the network. Specific approval must be obtained from the CEO before connecting any equipment to the Company's network. Where sensitive and/or confidential information, including Special Personal Information, are in transit over the network, such information will be encrypted in transit.

7.8. **Operating System Access Control**

7.8.1. Access to the Company's operating systems is controlled by a secure login process. The access control management procedure defined in clause 7.1 must be applied. The login procedure must also be protected by:

7.8.1.1. not displaying any previous login information (for example, the username in question);

7.8.1.2. limiting the number of unsuccessful attempts and locking the account if exceeded;

7.8.1.3. the password characters being hidden by symbols; and

7.8.1.4. displaying a general warning notice that only authorised Users are allowed.

7.8.2. All access to the Company's operating systems will be via a unique login identity ("ID") that will be audited and can be traced back to each individual User. The login ID must and will not give any indication of the level of access that it provides the User in question to the system (such as administration rights, for example).

7.8.3. System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

8. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

10. POLICY AWARENESS AND UPDATE

10.1. **Training and awareness:** The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

10.2. **Dissemination:** This Policy will be made available on the Company's network, intranet or similar portals.

10.3. **Review:** This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Information Quality Policy

1. SCHEDULE
2. INTRODUCTION
3. PURPOSE
4. SCOPE
5. POLICY
6. AREAS AND TIMELINES
7. RIGHTS RESERVED BY THE COMPANY
8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
9. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. The Company set out in item 1.1 of the Schedule ("**Company**") collects, processes, stores and archives personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 ("**POPIA**") in various facets of its business.

2.2. The information quality principal is one of the 8 (Eight) lawful processing principals set out in POPIA.

2.3. Certain areas of the business, in particular where the completeness and accuracy of Personal Information is vital, require that such Personal Information be updated on a regular basis.

3. PURPOSE

This information quality policy ("**Policy**") identifies the areas within the Company where Personal Information needs to be kept complete, accurate and up to date and where the Company must ensure that such information is not misleading.

4. SCOPE

4.1. This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**").

4.2. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in POPIA, such terms will be given the meaning ascribed to them in POPIA.

5. POLICY

5.1. The Company must and will update Personal Information on a regular defined timeline that will ensure that all Personal Information that is processed by the Company is complete, accurate and up to date. Such updates will also assist in ensuring that any Personal Information is not misleading. This procedure will facilitate the Company's compliance with the information quality principle of lawful processing set out in POPIA.

5.2. When reference is made to Personal Information being "complete" in this Policy, the Company will seek to ascertain whether all relevant data pertaining to Personal Information is captured on the Company's systems. In determining whether Personal Information is accurate, the Company will put processes in place in order to validate such information. For example, validation rules can be applied to ensure that there are no numbers in the name and surname fields provided in relation to a data subject, and likewise that there are no letters in the telephone number fields provided in relation to a data subject.

5.3. The purpose of collecting and processing the Personal Information by the Company will be kept in mind when determining the timeline for updating such information.

6. AREAS AND TIMELINES

6.1. The following has been identified by the Company as areas requiring compulsory, regular updates to Personal Information processed by the Company. The timelines required for updates are also set out below:

6.1.1. The Company's human resource and payroll system contains Personal Information (much of which is sensitive in nature) and such information must be updated every 3 (Three) months by way of questionnaire to Users who are employees of the Company;

6.1.2. Creditors added to any system may contain Personal Information and must be updated every 12 (Twelve) months; and

6.1.3. Debtors added to any system may contain Personal Information and must be updated on an ad hoc basis, as and when required.

7. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

9. POLICY AWARENESS AND UPDATE

9.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

9.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

9.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Backup and Restoration Policy and Procedure

1. SCHEDULE
2. BACKUP SCHEDULE
3. RETENTION PERIOD SCHEDULE
4. INTRODUCTION
5. OBJECTIVE
6. SCOPE
7. TERMS AND ABBREVIATIONS
8. DOCUMENTS
9. POLICY
10. PROCEDURE
11. RIGHTS RESERVED BY THE COMPANY
12. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
13. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF
1.2	Registration number : 1993/003391/08
1.3	VAT registration number : 4030108080
1.4	Physical address
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806
1.5	Email address : ceo@grootconstantia.co.za

2. BACKUP SCHEDULE

System/device	Location	Type of Backup	Frequency	Person responsible for Backup

3. RETENTION PERIOD SCHEDULE

System/device	Location	Type of Backup	Retention period

4. INTRODUCTION

4.1. The Company set out in item 1.1 of the Schedule ("**Company**") is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

4.2. The Backup and Restoration of data is an important aspect to ensure the availability of information / data for the Company.

5. OBJECTIVE

The objective of this policy and procedure ("**Policy**") is to formalise the Backup and Restoration process adopted by the Company. The process of Backing up data is pivotal to a successful disaster recovery plan ("**DRP**").

6. SCOPE

6.1. This Policy applies to (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**").

6.2. This Policy covers all servers, workstations, network devices, operating systems, applications and other information assets belonging to the Company.

7. TERMS AND ABBREVIATIONS

7.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Company makes use of the following terms:

7.1.1. **"Backup"** means the copying of physical or virtual files or databases to a secondary location for preservation to assist in the event of equipment failure or catastrophe;

7.1.2. **"Restoration"** means the process of restoring something to its former condition and, in the case of a computer or other electronic device, means returning it to a previous state, including (i) restoring a previous system backup or the original factory setting, or (ii) restoring data that was on the system;

7.1.3. **"CIO"** means the chief information officer of the Company; and

7.1.4. **"IT User"** means a User within the Company authorised to be responsible for the carrying out of the Company's necessary information technology ("**IT**") functions.

7.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

8. DOCUMENTS

This Policy should be read in conjunction with the Company's Acceptable Usage Policy insofar as it relates to IT aspects.

9. POLICY

9.1. The extent, frequency and retention period of Backups must reflect:

9.1.1. the Company's business requirements;

9.1.2. the Company's security requirements of the information involved;

9.1.3. how critical the information is to the Company's continued business operations;

9.1.4. the retention period for essential business information; and

9.1.5. any requirement for archived copies to be permanently retained by the Company.

9.2. The extent, frequency and retention periods of the Backups must be reviewed regularly and in each case where circumstances change or failures occur.

9.3. Backup arrangements must meet the requirements of the Company's business continuity plans.

9.4. The Company's critical systems must be clearly identified and, for such systems, the Backup arrangements must cover all system information, applications, and data necessary to recover the complete system in the event of a disaster.

9.5. Where Backup arrangements are automated, such automated solutions must be sufficiently tested prior to implementation and at regular intervals thereafter.

9.6. All Backup media must be appropriately labelled with dates and codes / markings which enables easy identification of the original source of the data and the type of Backup used on the media.

9.7. Where the confidentiality of the information is important, Backups must be protected by encryption and all encryption keys must be kept securely at all times, with clear procedures in place to ensure that Backup media can be promptly decrypted as required.

9.8. Accurate and complete records of the Backup copies must be retained both locally and remotely and afforded the same level of physical and environmental protection as other important documentation. Such records should include information pertaining to the department in question, data location, date of Backup, type of Backup and the like.

9.9. Copies of Backup media must be removed from all Company devices as soon as reasonably possible when a Backup or Restoration has been completed.

9.10. Backup media which is retained on-site at the Company, prior to being sent for storage at a remote location, must be stored securely at a sufficient distance away from the original data source to ensure that both the original and Backup copies are not compromised.
9.11. Access to the retained Backup media must be restricted to authorised staff only.
9.12. All Backups identified for long term storage must be stored at a secure remote location with appropriate environmental control and protection to ensure continuing media integrity.
9.13. Backup media must be protected in accordance with the Company's physical, environmental, data protection and media handling policies and procedures.
9.14. Restoration processes must be checked and tested regularly to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
9.15. Hard copy paper files containing important information and data must also be digitised and stored in a location where they will be Backed up by the Company in the same manner as electronic information.
9.16. Where Backups fail, data and system owners must be promptly informed and a record maintained. Such a record must include information regarding any action taken by the Company to address such failure.
9.17. Backup data / media no longer required must be clearly marked and recorded for secure disposal or destruction, with due environmental consideration.
9.18. Where provision is made in this Policy for reviews to be done at regular intervals, such intervals will be determined by the CIO in his / her sole discretion.

10. PROCEDURE

10.1. There are 5 (Five) common types of backup, they are:
10.1.1. **Full Backup**: A full Backup is when every single file and folder in the Company's systems is Backed up. A full Backup takes longer and requires more space than other types of Backups. However, the process of Restoring lost data from the Backup is much faster.
10.1.2. **Incremental Backup**: With incremental Backups only the first Backup is a full Backup. Subsequent Backups only store changes that were made after the previous Backup. The process of Restoring lost data from the Backup is longer, however, the Backup process itself is much quicker.
10.1.3. **Differential Backup**: A differential Backup is similar to an incremental Backup. With both, the first Backup is full and subsequent Backups only store changes made to files after the last Backup. This type of Backup requires more storage space than an incremental Backup does, however, it also allows for a faster Restoration time.
10.1.4. **Mirror Backup**: A mirror Backup is when an exact copy is made of the source data. The advantage of mirror Backups as opposed to full, incremental, or differential Backups, is that old, obsolete files are not being stored. When obsolete files are deleted, they are also deleted from the mirror Backup when the system Backs up. The disadvantage of a mirror Backup is that, if files are accidentally deleted, they may also be lost from the Backup if the deletion is not discovered prior to the next scheduled Backup.
10.1.5. **Replication Backup**: A replication Backup occurs where data stored on servers is replicated between different servers. Sometimes these servers may be in the same data centre. If the Backup is a pure replication, there is a risk that if the data on the main server is corrupted, the rest of the replicated data could also be corrupted. When implementing replication Backups, a Backup that is at least 1 (One) day older than the live data must be kept to manage this risk.
10.2. **Backup schedule**: Item 2 of the Schedule sets out the Backup schedule of the Company, which must be reviewed and updated on a regular basis. Item 2 includes the following information:
10.2.1. The system / device to be Backed up;
10.2.2. The location of such device;
10.2.3. The type of Backup that was implemented, including:
10.2.3.1. full Backup;
10.2.3.2. incremental Backup;
10.2.3.3. differential Backup;
10.2.3.4. mirror Backup; and / or
10.2.3.5. replication Backup;
10.2.4. The frequency of the Backup; and
10.2.5. The person responsible for the Backup.
10.3. **Retention period of Backups**: Item 3 of the Schedule sets out the retention periods of Backups implemented within the Company. This schedule must be reviewed and updated on a regular basis. Item 3 includes the following information:
10.3.1. The system/device Backed up;
10.3.2. The location of such device;
10.3.3. The type of Backup that was implemented, including:
10.3.3.1. full Backup;
10.3.3.2. incremental Backup;
10.3.3.3. differential Backup;
10.3.3.4. mirror Backup; and / or
10.3.3.5. replication Backup; and
10.3.4. The retention period of the Backup in question.
10.4. **IT Users responsibilities**
10.4.1. IT Users must ensure that data is securely maintained and is available for Backup at all times.
10.4.2. IT Users must store any data / files that require Backup on their allocated network storage area and not on local hard drives.
10.4.3. If the allocated storage area becomes unavailable, IT Users may not temporarily save the data locally on hard drives or on a USB data stick, but must promptly contact the CIO to Restore the data in question.

10.5. **Data Restoration**

10.5.1. Data (file) Restoration must only be done by competent, authorised staff within the Company.

10.5.2. The following procedure must be followed when performing Restorations:

10.5.2.1. IT Users must request the Restoration of data by contacting the CIO;

10.5.2.2. The CIO must verify that the IT User has permission or authorisation to view or Restore data prior to any Restoration taking place;

10.5.2.3. The CIO must request the following information from the IT User in order to facilitate the Restoration:

10.5.2.3.1. The reason for the Restoration;

10.5.2.3.2. The names of files or folders to be Restored;

10.5.2.3.3. The original location of the files or folders to be Restored;

10.5.2.3.4. The IT User's best estimation of the date and time when the IT User noticed the deletion / corruption in question; and

10.5.2.3.5. The IT User's best estimation of the date and time when the IT User recalls the files or folders in question being accessible and intact;

10.5.2.4. Requests from third party software / hardware vendors for file or system Restorations for the purpose of system support, maintenance, testing or other unforeseen circumstance must be made to the CIO;

10.5.2.5. IT Users accessing Backup media for the purpose of a Restoration must ensure that any media used is returned to a secure location when it is no longer required; and

10.5.2.6. A log must be maintained to record the use of Backup media whenever it has been requested and / or removed from secure storage.

11. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of the Promotion of Access to Information Act 4 of 2013 ("POPIA"). Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

12. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

13. POLICY AWARENESS AND UPDATE

13.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

13.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

13.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Information Security Policy

1. SCHEDULE
2. INTRODUCTION
3. OBJECTIVE
4. SCOPE
5. TERMS AND ABBREVIATIONS
6. DOCUMENTS
7. POLICY
8. RESPONSIBILITIES IN RELATION TO INFORMATION SECURITY
9. RIGHTS RESERVED BY THE COMPANY
10. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
11. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. All organisations that process any information that identifies an individual or juristic entity must implement information security measures.

2.2. Information security measures that are implemented will depend on the type of information that is processed. Information security measures effectively mean the processes and methodologies that are designed and implemented by an organisation to protect (i) printed, (ii) electronic, and / or (iii) any other form of sensitive or confidential information ("**Confidential Information**") and / or Personal Information (as defined below) from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

2.3. This policy and procedure document ("**Policy**") regulates the information security measures implemented by the Company set out in item 1.1. of the Schedule ("**Company**").

2.4. Where the information being processed comprises personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 ("**Personal Information**"), the provisions of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") will apply to the processing of such information by or on behalf of the Company.

3. OBJECTIVE

The objective of this Policy is to (i) regulate and formalise the information security environment of the Company, (ii) set out the various responsibilities of persons in the information security environment, and (iii) reference the related policies and procedures that will assist in improving information security in, or in relation to, the Company. It is important to ensure that information security measures address the confidentiality, integrity and availability of information.

4. SCOPE

This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**") that create and / or use records that relate to the Company's business operations.

5. TERMS AND ABBREVIATIONS

5.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Company makes use of the following terms:

5.1.1. "**ISO27000 Series**" means the international standard for implementing an information security management system; and

5.1.2. "**GDPR**" means the general data protection regulation of the European Union.

5.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

6. DOCUMENTS

6.1. This Policy should be read in conjunction with the following related policies and procedures of the Company, and any other policies and procedures that regulate data protection that the Company may implement in the future:

6.1.1. Acceptable Use Policy;

6.1.2. Access Management and Control Policy and Procedure;

6.1.3. Backup and Restoration Policy and Procedure;

6.1.4. Bring Your Own Device Policy;
6.1.5. Clean Desk and Clear Screen Policy;
6.1.6. Information Incident Management Policy and Procedure;
6.1.7. Information Privacy Policy and Framework;
6.1.8. Information Transfer Policy and Procedure;
6.1.9. Information Quality Policy;
6.1.10. Physical and Environmental Security Policy and Procedure;
6.1.11. Retention and Destruction Policy; and
6.1.12. Vulnerability and Penetration Testing Policy.

7. POLICY

7.1. The Company will apply the measures necessary to ensure the confidentiality, integrity and availability of (i) Confidential Information, and / or Personal Information. The Company will apply the ISO27000 Series in, or in relation to, its business practices.
7.2. The Company will further identify Personal Information and ensure that the information is protected in accordance with the requirements required by POPIA and / or the GDPR (if applicable).
7.3. Where the Personal Information in question is more sensitive in nature, such as information pertaining to minors, health and sex life ("**Special Personal Information**"), the Company will ensure that any more stringent measures required under POPIA and / or the GDPR in relation to the processing of such information are implemented.

8. RESPONSIBILITIES IN RELATION TO INFORMATION SECURITY

8.1. The various responsibilities in terms of this Policy must be allocated throughout the Company and Users will be categorised as follows:
8.1.1. **Accountable**: a User who will be ultimately accountable in the event of a breach or contravention of this Policy;
8.1.2. **Responsible**: a User who is responsible for the management and implementation of this Policy;
8.1.3. **Supportive**: a User who assists in implementing this Policy;
8.1.4. **Consulted**: a User who is consulted for advice and information regarding this Policy; and
8.1.5. **Informed**: a User who must and will be informed and given information regarding this Policy.
8.2. The responsibilities in terms of this Policy must be formalised in a (i) Responsible, (ii) Accountable, (iii) Supporting, (iv) Consulted and (v) Informed ("**RASCI**") Matrix and must be written into the job descriptions and / or contractual obligations, as the case may be, of the individual Users.

9. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

10. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

11. POLICY AWARENESS AND UPDATE

11.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.
11.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.
11.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Physical and Environmental Security Policy

1. SCHEDULE
2. INTRODUCTION
3. PURPOSE
4. SCOPE
5. RELATED DOCUMENTS
6. POLICY
7. KEY PRINCIPLES
8. RIGHTS RESERVED BY THE COMPANY
9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
10. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

This policy ("**Policy**") sets out the requirements for protecting the information and technology resources and assets belonging to the Company set out in item 1.1 of the Schedule ("**Company**") from physical and environmental threats in order to reduce the risk of (i) loss, theft, damage and / or unauthorised access to those resources, or (ii) interference with, and disruption to, the Company's operations.

3. PURPOSE

The purpose of this Policy is to ensure that the Company implements measures focused on the physical and environmental control measures put in place to protect the Company's information and technology resources and assets.

4. SCOPE

4.1. This Policy applies to all departments and functions that use information and technology resources and assets to create, access, update, store, maintain and / or manage information or data to perform their business functions. This information includes personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 ("**POPIA**").

4.2. This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**").

4.3. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in POPIA, such terms will be given the meaning ascribed to them in POPIA.

5. RELATED DOCUMENTS

This Policy is read together with the other policies of the Company that regulate the use and protection of the Company's assets, including its information. In the event of any inconsistency between this Policy and other policies of the Company, the policy that provides the greatest protection to the Company and its assets will prevail.

6. POLICY

All Users and the Company's property, information and technology resources and assets should have appropriate physical and environmental security controls applied to mitigate the identified and potential information security risks to these assets. Such risks include (i) fire, natural disasters, burglary, theft, vandalism, and terrorism (physical security risks), and (ii) electrical surges, flooding and natural disasters (environmental security risks).

7. KEY PRINCIPLES

7.1. **Risk assessment and treatment**

7.1.1. A security risk assessment of physical and environmental threats to Users, property, information and technology resources and assets of the Company must be conducted on an annual basis, unless required more frequently in terms of any other policy of the Company. Based on the outcome of the risk assessment conducted, appropriate key controls must be implemented by the Company to mitigate the risk.

7.2. **Physical security**

7.2.1. Appropriate physical security measures must be identified in relation to the type of information or data that is required to be protected. For example, where there is an area within the Company's premises that visitors can access, but where no (i) Personal Information, and / or (ii) sensitive, confidential, proprietary and / or critical information of the Company ("**Confidential Information**") is kept, a lower level of physical security will be required than for an area where (i) Personal Information, and / or (ii) Confidential Information is stored or otherwise processed by the Company. A map of the Company's premises ("**Premises**") will be provided. This will then be colour-coded into areas that are either low, medium or high risk. Appropriate physical controls must then be implemented in relation to all areas within the Premises. The areas in the Premises should be classified as follows:

7.2.1.1. Public areas such as the reception, the canteen, the boardrooms in the open areas may be classified as a low risk;

7.2.1.2. Controlled areas such as general working areas or boardrooms within these working areas may be classified as a medium risk; and

7.2.1.3. Highly restricted areas such as the information technology department, server room, finance department, human resources department and other areas where (i) Personal Information, and / or (ii) Confidential Information are processed may be classified as high risk.

7.2.2. Physical security measures must be implemented which will include:

7.2.2.1. Security guards at the entrance where visitors enter the premises;

7.2.2.2. An armed response that can be activated in the case of an emergency;

7.2.2.3. Alarm systems that will be activated when the building is unoccupied to ensure intrusion detection;

7.2.2.4. Cameras at strategic points to ensure that activities are monitored, recorded and stored;

7.2.2.5. Physical Access control, including a reception area where visitors must report before accessing the controlled areas; and

7.2.2.6. Controlled access by employees and authorised third parties.

7.2.3. Network wiring and equipment rooms and cabinets must be locked when unattended with access limited only to authorised personnel (typically network support staff) and visitors escorted by such authorised personnel. Other network cabling and devices should likewise be physically secured where feasible. Core network facilities must have the date and time of all entry and departure recorded.

7.2.4. All office doors must remain locked after hours or when offices are unattended for a period of time.

7.2.5. Mobile storage devices must be stored securely when unattended.

7.2.6. For purposes of this Policy, appropriate secure storage methods include (i) a locking security cable attached directly to the device in question, such as laptops, (ii) storage in a locked cabinet or closet, or (iii) storage in a locked office.

7.2.7. Encrypting data stored on mobile devices, such as whole disk encryption on laptop computers, reduces the risk of a breach of data resulting from theft, loss, or unauthorised access. When Users travel with mobile storage devices or use them in public places, appropriate security precautions must be taken to prevent loss, theft, damage, or unauthorised access to such devices. This includes, at the discretion of the management of the Company, the use of tracking and recovery software on laptop computers.

7.3. **Environmental security**

7.3.1. The possible threat of the environment on Users, property, and information and technology resources and assets of the Company must be assessed on an annual basis, unless required more frequently in terms of any other policy of the Company. Based on the outcome of the risk assessment, appropriate key controls must be implemented to mitigate the risk. Some potential risks include, without limitation:

7.3.1.1. **Water**: areas where there is a risk of water damage due to flooding or bursting of geysers should be identified. Servers and other sensitive equipment that contain (i) Personal Information, and / or (ii) Confidential Information should be kept away from these areas.

7.3.1.2. **Electrical power**: electrical power for servers hosting (i) Personal Information, and / or (ii) Confidential Information must be protected by uninterruptable power supplies to (i) ensure the continuity of services during power outages, and (ii) protect equipment from damage due to power irregularities. Systems hosting such information must also be protected with a standby power generator where reasonably possible.

7.3.1.3. **Natural disasters**: all conceivable threats should be identified and mitigating controls should be put in place. An example of a control could be to install lightning equipment to prevent lightning from causing damage to the building that the Company occupies.

7.4. **Incident Management**

7.4.1. An incident log of all physical and environmental breaches must be kept. The incident log must indicate the (i) type of incident, and (ii) action that has been taken by the Company to manage the incident.

7.4.2. Furthermore, a log of all evidence gathered during any investigation regarding the cause and damage sustained as a result of any physical or environmental threat must be kept and stored in a secure folder.

8. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

10. POLICY AWARENESS AND UPDATE

10.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

10.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

10.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Bring Your Own Device (BYOD) Policy

1. SCHEDULE
2. INTRODUCTION
3. PURPOSE
4. SCOPE
5. REFERENCE DOCUMENTS
6. POLICY
7. PROCEDURES
8. RIGHTS RESERVED BY THE COMPANY
9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
10. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. Bring your own Device ("**BYOD**") is the practice of allowing employees and other authorised persons that perform work for the Company set out in item 1.1 of the Schedule ("**Company**") to use their own personal devices for work purposes. This includes, without limitation, mobile phones, laptops and tablets. The use of such personal devices for Company purposes will be referred to as BYOD, or the BYOD initiative, for purposes of this Policy.

2.2. It is imperative for the Company to protect and secure the data or information that it processes, both for reputational reasons and to ensure compliance with the provisions of the (i) Protection of Personal Information Act no. 4 of 2013 ("**POPIA**"), applicable to the processing of personal information, as this term is defined in POPIA ("**Personal Information**"), in South Africa, and / or (ii) General Data Protection Regulation of the European union, that will apply where the personal information of European citizens is processed by the Company.

3. PURPOSE

The purpose of this policy ("**Policy**") is to set out how the Company will retain control over its information while such information is being accessed through devices that are not owned by the Company.

4. SCOPE

This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**") that make use of personally-owned devices to process, store or transfer any information for purposes of conducting business for the Company. This Policy applies to all Users irrespective of whether they make use of personal devices for Company business at the premises of the Company ("**Premises**") or remotely.

5. REFERENCE DOCUMENTS

This policy should be read in conjunction with other Company policies that regulate the security of information including, without limitation, the Acceptable Usage Policy.

6. POLICY

6.1. The Company supports the use of BYOD for work purposes. The Company restricts the use of BYOD only to a limited number of Users who would not otherwise be in a position to perform the work, after proper authorisation, from the chief information officer of the Company ("**CIO**"), has been obtained.

6.2. All information belonging to the Company that is stored, transferred or processed on BYOD devices remains under the Company's ownership at all times, and the Company retains the right to regulate such information, and the processing of it, even though it is not the owner of the BYOD.

7. PROCEDURES

7.1. **Permitted use of BYOD**

7.1.1. The CIO will create a list of Users with (i) job titles, in the event that Users are employees, or (ii) "relationship to Company", in the event that Users are not employees, who are authorised to use BYOD, together with the applications and / or databases they are allowed to access with their own personal device;

7.1.2. A User's request for access (using a mobile users access form) to participate in the BYOD initiative must be formally completed, and must be authorised by the CIO in writing before any access is granted to such User; and

7.1.3. Only Users that need information to perform their duties effectively with a BYOD device will be granted permission to use their own devices in terms of this Policy.

7.2. **Permitted devices**

7.2.1. The CIO will create and maintain a list of acceptable devices which can be used as BYOD, together with mandatory settings to be deployed for each device.

7.3. **Acceptable usage**

7.3.1. In addition to all of the provisions contained in the Acceptable Usage Policy, which also apply to this Policy, the following requirements are mandatory for every BYOD User:

7.3.1.1. Users must set and use a strong passcode to access personal devices;

7.3.1.2. Users must not share passcodes with anyone else;

7.3.1.3. Users must set devices to lock automatically when the device is inactive for more than 1 (One) minute;

7.3.1.4. The latest and most secure antivirus software must be installed on each device and updated regularly;

7.3.1.5. Patches and updates to operating systems of devices must be installed regularly;

7.3.1.6. Each device must be configured to enable the device in question to be remotely-wiped should it be misplaced;

7.3.1.7. Personal Information, and / or sensitive, critical, confidential and / or proprietary information of the Company ("**Confidential Information**") must be protected by the most stringent security measures available (such as two pin authentication);

7.3.1.8. When using BYOD off the Premises, Users must ensure that all devices are not left unattended and, if possible, these should be physically locked away;

7.3.1.9. When using BYOD in public places, Users must ensure that no Company information can be read by unauthorised persons; and

7.3.1.10. Users must notify the CIO before any device used in the BYOD initiative is being disposed of, sold and / or handed to a third party for servicing.

7.4. **Prohibited uses of BYODs**

7.4.1. BYOD Users are prohibited from doing the following with devices used in the BYOD initiative:

7.4.1.1. Allow anyone else access to the device in question;

7.4.1.2. Install unknown and untrusted applications;

7.4.1.3. Store illegal material on the device;

7.4.1.4. Install unlicensed software;

7.4.1.5. Connect via Bluetooth to any unknown devices;

7.4.1.6. Connect to unknown wifi networks;

7.4.1.7. Locally store passwords;

7.4.1.8. Configure logins to save passwords for applications;

7.4.1.9. Locally store any information that is (i) Personal Information, and / or (ii) Confidential Information; and

7.4.1.10. Transfer any Company information to any unauthorised devices, including private / home devices.

7.5. **Special rights**

7.5.1. The Company has the right to view, edit, and delete all Company information that is stored, transferred or processed on a BYOD without the consent of the owner of the device in question.

7.6. **Reimbursement**

7.6.1. The Company will pay for the following:

7.6.1.1. Software required by the Company in order to manage and control Company related information stored on any authorised device; and

7.6.1.2. Other approved applications required to fulfil the duties or responsibilities of the relevant User.

7.7. **Security breaches**

7.7.1. All security breaches related to the BYOD initiative must be reported immediately to the CIO.

7.7.2. All security or other related weaknesses that Users become aware of that have not yet become security incidents or breaches must be reported to the CIO by the User within 24 (Twenty-Four) hours of the User becoming aware of any such weakness.

8. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

10. POLICY AWARENESS AND UPDATE

10.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

10.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

10.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Information Transfer Policy

1. SCHEDULE
2. INTRODUCTION
3. PURPOSE
4. SCOPE AND USERS
5. REFERENCE DOCUMENT
6. POLICY
7. RESPONSIBILITIES OF THE SENDER AND RECEIVER OF INFORMATION
8. RELATIONSHIP WITH EXTERNAL PARTIES
9. RIGHTS RESERVED BY THE COMPANY
10. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
11. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. This policy regulates the transfer of information within and from and to the Company set out in item 1.1. of the Schedule ("**Company**").

2.2. Where the information being transferred comprises personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 ("**Personal Information**"), the provisions of POPIA will apply to the processing of such information by or on behalf of the Company.

3. PURPOSE

3.1. There are many occasions when information is transferred between different departments of the Company, and between the Company and third-party service providers, clients, customers and the like. This transfer of information is effected by a wide variety of media and methods, in both electronic and paper format. In every transfer of information, there is a risk that the information in question may be lost, misappropriated or accidentally disclosed. Where the information in question is (i) Personal Information, and / or confidential, sensitive, critical or proprietary information of the Company ("**Confidential Information**") the risk to the Company increases significantly.

3.2. The Company often has a duty of care in handling information. For this reason, and because of its legal obligations under POPIA, the Company considers it imperative to maintain the trust of its stakeholders and partners. It is, therefore, essential that the transfer of information is performed in a way that adequately protects such information.

3.3. It is at all times the responsibility of the sender of information to assess the risks involved in the transfer of such information and to ensure that adequate controls are in place to mitigate such risks. Where the sender of information delegates the final actual task of sending information to untrained or inexperienced staff, the original sender remains responsible for ensuring that the transfer of information complies with this Policy. This Policy outlines the responsibilities attached to, and the minimum-security requirements, for the transfer of information, including (i) Personal Information, and / or (ii) Confidential Information.

4. SCOPE AND USERS

4.1. This policy applies to all departments where (i) Personal Information, and / or (ii) Confidential Information is created, accessed, processed, updated, stored, maintained or managed.

4.2. This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**") who are in any way involved in the transfer of information as contemplated by this Policy.

4.3. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in POPIA, such terms will be given the meaning ascribed to them in POPIA.

5. REFERENCE DOCUMENT

This policy should be read in conjunction with the Company's other policies that regulate the security of information, including, without limitation, the Acceptable Usage Policy.

6. POLICY

6.1. **Electronic communication channels**

6.1.1. The Company's information may be exchanged through the electronic communication channels outlined below.

6.1.2. New data channels must be approved by the chief information officer of the ("**CIO**") the Company prior to being implemented. A data channel is either a physical transmission medium, such as a wire transfer, or a logical connection over a multiplexed medium, such as a radio channel ("**Data Channel**"). The CIO's approval will set out the (i) type of communication allowed, and (ii) controls pertaining to the use of the Data Channel. Public information may be made available to the public, but all information meant for internal use only may only be transferred to parties that are authorised by the Company to receive such information and that are bound contractually not to disclose such information, whether by employment agreements or appropriate non-disclosure agreements.

6.1.3. Where the information is classified as either (i) Personal Information, and / or (ii) Confidential Information, the relevant Data Channels and other guidelines set out below should be used to ensure that such information is transferred in a secure manner and that only certain secure channels are used to transfer such Information.

6.1.3.1. Email may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when such information has been sufficiently password protected or properly encrypted in the email in question;

6.1.3.2. A file transfer method may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when a secure file transfer protocol (known as a "**SFTP**") channel is used;

6.1.3.3. Portable Media (such as CDs, DVDs, USB drives and memory cards) may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when such information on the device in question is properly password protected or encrypted; and

6.1.3.4. Telephonic communication, fax transmission, mobile voice or sms communication, and / or social media may not be used to transfer or disclose (i) Personal Information, and / or (ii) Confidential Information.

6.2. **Non-electronic communication channels**

6.2.1. The Company's information may be exchanged through the non-electronic communication channels outlined below.

6.2.2. Public information may be made available to the public, but all information meant for internal use only may only be transferred to parties that are authorised by the Company to receive such information and that are bound contractually not to disclose such information, whether by employment agreements or appropriate non-disclosure agreements.

6.2.3. Where the information is classified as either (i) Personal Information, and / or (ii) Confidential Information, the guidelines set out below should be used to ensure that such information is transferred in a secure manner and that only certain secure channels are used to transfer such Information.

6.2.3.1. Registered or normal post may not be used to transfer (i) Personal Information, and / or (ii) Confidential Information; and

6.2.3.2. Letters delivered by hand may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when the sender of such information ensures that the party receiving the information is properly identified and authorised to receive such information.

7. RESPONSIBILITIES OF THE SENDER AND RECEIVER OF INFORMATION

7.1. The sender's responsibilities for transferring (i) Personal Information, and / or (ii) Confidential Information are:

7.1.1. assessing the information to be sent and ensuring that it is in line with the guidelines set out in this Policy;

7.1.2. ensuring that the identity of the receiver is known, that such receiver is authorised to receive the information and that the channel used for the transfer is conducive to transfer the information to that person;

7.1.3. ensuring that the transfer of information is formally confirmed and documented; and

7.1.4. ensuring that the information is sent and tracked in an appropriate manner to ensure compliance with this Policy.

7.2. The person receiving (i) Personal Information, and / or (ii) Confidential Information is responsible for ensuring that:

7.2.1. the information received is information that they have a right to receive; and

7.2.2. they fully disclose their identity.

8. RELATIONSHIP WITH EXTERNAL PARTIES

8.1. Before exchanging any information with any person or party outside of the Company, an agreement must be concluded between the Company and such third party. Such agreement must comply with POPIA and must contain at least the following clauses:

8.1.1. Method of identification of the third party;

8.1.2. Confirmations or warranties regarding authorisation to access information;

8.1.3. Technical standards and appropriate Data Channels for the transfer of information;

8.1.4. Labelling and handling of (i) Personal Information, and / or (ii) Confidential Information;

8.1.5. Warranties from the third party regarding compliance with POPIA and all other relevant privacy laws;

8.1.6. Obligations on the third party to safeguard the security of the information in question;

8.1.7. Indemnities in favour of the Company in the event of a breach by the third party of POPIA or the agreement itself;

8.1.8. Protections for the Company's intellectual property rights; and

8.1.9. Incident responses and what must be done in the event of security breaches.

9. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in **such a way** that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

10. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

11. POLICY AWARENESS AND UPDATE

11.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

11.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

11.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Clean Desk and Clear Screen Policy

1. SCHEDULE
2. INTRODUCTION
3. PURPOSE
4. SCOPE
5. RELATED DOCUMENTS
6. DEFINITIONS
7. POLICY
8. RIGHTS RESERVED BY THE COMPANY
9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
10. POLICY AWARENESS AND UPDATES

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. In the event that (i) personal information, as this is defined in the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), and / or (ii) other confidential, sensitive or restricted information, is not securely stored away when not directly in use, the Company set out in item 1.1 of the Schedule ("**Company**") could be at risk of suffering a data breach, which can cause it reputational and other damage.

2.2. All (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**") are required to keep their (i) their Desks and Tables, and (ii) Screens clear of all personal information in terms of POPIA ("**Personal Information**") and / or confidential, sensitive and / or proprietary information belonging to the Company ("**Confidential Information**") when such information is not being used or accessed by the User in question.

3. PURPOSE

3.1. The purpose of this policy ("**Policy**") is to ensure that all paper and electronic records containing Personal Information and / or any other Confidential Information are suitably secured when not in use and are not left visible on an unattended (i) Desk and Table, or (ii) Screen.

3.2. This Policy applies to all working areas, including Desks and Tables, which must not have any Personal Information and / or Confidential Information displayed on them whilst unattended for any period of time. In the event that the User in question is working on any Company system or device remotely, such User must also ensure that the provisions of this Policy are strictly adhered to at all times.

3.3. Controlling physical access to the information assets within the Company is vitally important. This relies upon physical, technological and policy Controls to ensure that the Company operates within a secure environment at all times, protecting personnel, facilities, information and data from the risk of:

3.3.1. loss or damage of information resources;

3.3.2. unauthorised access to information resources;

3.3.3. disruption and / or destruction of information processing facilities; and

3.3.4. breach of relevant legislation, including POPIA, and / or non-compliance with regulatory standards.

4. SCOPE

This Policy applies to all Users, and any and all functions and departments within the Company where Personal Information and / or Confidential Information are created, accessed, updated, stored, maintained, managed or even deleted.

5. RELATED DOCUMENTS

This Policy is to be read together with the Company's Acceptable Usage Policy, which also deals with the Company's information security policies and procedures.

6. DEFINITIONS

6.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Company makes use of the following terms:

6.1.1. "**Controls**" means control measures put in place by the Company to mitigate the risks identified to the security of Personal Information and / or Confidential Information, including instituting and implementing policies and procedures, management control, reporting, physical security measures and the like;

6.1.2. "**Desk/s and Table/s"** means any physical working area where Personal Information and / or Confidential Information is processed, including printing areas, whether situated at the Company's premises or remotely; and

6.1.3. "**Screen/s**" means any monitor on any device upon which Personal Information and / or Confidential Information is stored that displays such information.

6.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

7. POLICY

7.1. All Users are required, and undertake, to apply a (i) clean Desk and Table, and (ii) clear Screen policy, as this will help to protect the Company's information assets from being compromised in any way. Without detracting from the generality of the aforegoing obligations on Users in terms of this Policy, the following actions must be taken to ensure that the necessary Controls are in place:

7.1.1. Users must ensure that all Personal Information and / or Confidential Information stored in both hardcopy or electronic form is secured in their Desk and Table at the end of each day and when they are expected to be away from their Desk and Table;

7.1.2. Screens must be locked when a User's Desk and Table is unoccupied;

7.1.3. All Personal Information and / or Confidential Information, in whatever format this may be stored, must be locked in a drawer or cupboard at the end of each day and when the desk is unoccupied;

7.1.4. Filing cabinets containing Personal Information and / or Confidential Information must be kept closed and locked at the end of each day and when not in use or when unattended;

7.1.5. Keys used to access and Personal Information and / or Confidential Information must not be left at or on an unattended Desk and Table;

7.1.6. Laptops and computers must be either locked with a secure locking mechanism or locked away in a drawer or cabinet at the end of each work day or when they are left unattended;

7.1.7. Passwords may not be left on any sticky or other notes posted on or under a computer or laptop, nor may they be left written down in an accessible location;

7.1.8. Printouts containing any Personal Information and / or Confidential Information must be removed from the printer immediately;

7.1.9. All Personal Information and / or Confidential Information that is ready to be disposed of must be placed in the designated confidential disposal bins to be shredded or otherwise securely destroyed;

7.1.10. Whiteboards containing Personal Information and / or Confidential Information should be erased as soon as reasonably possible; and

7.1.11. All mass storage devices, including CDROMs, DVDs or USB drives must be treated as sensitive and must be secured in a locked drawer.

8. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

10. POLICY AWARENESS AND UPDATES

10.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

10.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

10.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Retention and Destruction Policy and Procedure

1. SCHEDULE
2. INTRODUCTION
3. OBJECTIVE
4. SCOPE
5. REREFENCE DOCUMENTS
6. PROCEDURES
7. RIGHTS RESERVED BY THE COMPANY
8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
9. POLICY AWARENESS AND UPDATE
10. ANNEXURE A

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF
1.2	Registration number : 1993/003391/08
1.3	VAT registration number : 4030108080
1.4	Physical address
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806
1.5	Email address : ceo@grootconstantia.co.za

2. INTRODUCTION

2.1. It is important to identify the time periods that information should be retained by the Company set out in item 1.1 of the Schedule ("**Company**"). A retention period is usually the minimum period that records of information must be retained. After the retention period has elapsed, such records must either be archived or destroyed.

2.2. It is also important not to retain information for longer than necessary. Where a retention period has expired, the record in question can be destroyed.

3. OBJECTIVE

The objective of this policy and procedure ("**Policy**") is to (i) determine the retention period of records that the Company keeps, and (ii) describe the process of destruction or archiving such records, where applicable.

4. SCOPE

4.1. This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**") that create and / or use records that relate to the Company's business operations.

4.2. This Policy applies to all records of information, whether in manual or electronic format.

4.3. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), such terms will be given the meaning ascribed to them in POPIA.

5. REREFENCE DOCUMENTS

This Policy should be read in conjunction with other policies of the Company that regulated the protection of personal information, as this term is defined in POPIA ("**Personal Information**").

6. PROCEDURES

6.1. **Records**

6.1.1. **Lifecycle of records**

6.1.1.1. The Company acknowledges that records have a lifecycle and that, if they have come to an end of their retention period, a decision should be made regarding archiving or destroying them.

6.1.1.2. The records management lifecycle is as follows:

6.1.1.2.1. The origination of the record is determined either by the creation of the record by the Company, or the receipt of the record by the Company from a compliant third party.

6.1.1.2.2. Once a record is created or received, it is used, updated, modified, stored, maintained and / or protected by the Company on a day to day basis.

6.1.1.2.3. At the end of the useful life of the record in question, or when required by relevant and applicable legislation, the Company must evaluate whether such record should be archived or destroyed.

6.1.2. **Retention of records**

6.1.2.1. Proper record management is an important part of doing business and the Company must ensure that it complies with all legislation that is applicable to the records held by it.

6.1.2.2. As there may be different retention periods depending on the nature of the record, the information set out below will assist in determining the applicable retention period for a record:

6.1.2.2.1. In the event that a minimum retention period is prescribed by legislation, then the retention period set out in such legislation applies.

6.1.2.2.2. In the event that there is no legislated retention period, the retention period set out in the Company's code of conduct ("**Code**") applies.

6.1.2.2.3. In the event that there is no retention period stipulated in the Code, or if the Company does not have a Code, then the retention period prescribed by any specific applicable contract or agreement applies.

6.1.2.2.4. In the event that there is no retention period stipulated in any specific contract or agreement, then any retention period agreed to by the Data Subject in question applies (and a Data Subject may agree to records of their Personal Information being held for longer periods of time than that prescribed by legislation or by the Company itself).

6.1.2.2.5. In the event that a Data Subject has not stipulated or consented to a specific retention period in respect of their records of Personal Information, then any retention period prescribed by the chief executive officer ("**CEO**") or compliance officer of the Company will apply.

6.1.2.2.6. In the event that none of the above apply, then the Company's information officer may determine the applicable retention period.

6.1.2.3. A table of retention periods are also set out in **Annexure A** for further guidance.

6.2. **Destruction**

6.2.1. **Destruction decision**

6.2.1.1. The destruction of records is not the same as the disposition of records.

6.2.1.2. The disposition of records refers to the wide range of actions undertaken to manage records over time, which may include the transfer of records to an archival storage.

6.2.1.3. The destruction of a record is the act of destroying a record permanently by obliterating such record, so that the information stored in it can no longer be physically or electronically reconstructed or recovered. Any decision to destroy a record must be formally approved by the CEO in writing.

6.2.1.4. Where the retention period for a record has expired, a decision must be made to either (i) continue to retain the document (if permitted by law), (ii) transfer the record to an archival storage, or (iii) destroy the record. Some of the factors that will influence this decision are:

6.2.1.4.1. whether the record reached its useful life;

6.2.1.4.2. could there be a future challenge where the record is needed in a civil or criminal case; and

6.2.1.4.3. does the record need to be retained for commercial or business purposes?

6.2.1.5. The abovementioned decision must be formally made and must be properly documented. Such decision must be in writing and must be signed off by the CEO.

6.2.2. **Destruction of paper records**

6.2.2.1. Where a formal decision has been made to destroy Company records, the destruction must be done securely. Paper records must either be shredded by the Company or placed in confidential bins to be removed by a reputable third-party provider.

6.2.2.2. Paper records must not be discarded in trash cans or destroyed by other unsecured methods.

6.2.3. **Destruction of electronic records**

6.2.3.1. Before electronic records are destroyed, archiving the records should be considered. If the decision is made to destroy the record, then one of the following techniques must be used:

6.2.3.1.1. **Overwriting**: Overwriting is an effective method of destroying electronic records. This method involves the use of software that overwrites the record multiple times (up to 10 (Ten) times) with strings of "1's" and "0's". This makes the possibility of recovering the record much more remote.

6.2.3.1.2. **Physically destroying storage media**: Physically destroying the storage media or record must be used where (i) Personal Information, and / or (ii) sensitive or confidential information of the Company is stored on a record. This is also the most appropriate method of destroying records stored on portable media, such as hard drives, and shredding CDs and DVDs.

7. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

9. POLICY AWARENESS AND UPDATE

9.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

9.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

9.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

10. ANNEXURE A

Information is only retained by the Company for as long as it there is a legitimate purpose for the information to be retained, or if there is a legal requirement to retain certain information. In some cases, a decision may be made by the Company to retain information for a specific period of time, even if there is no legislated retention period.

The following table sets out the retention periods of information that is held by the Company.

CATEGORIES OF RECORDS ON EACH SUBJECT	FORM HELD	RETENTION PERIOD
Company secretarial records		
Notice of Incorporation	Electronic and physical	Indefinite
Memorandum of Incorporation and alterations or amendments	Electronic and physical	Indefinite
Rules	Electronic and physical	Indefinite
Register of Company secretary and auditors	Electronic and physical	Indefinite
Notice of shareholders' meetings, including any resolutions adopted and reports presented at an AGM	Electronic and physical	7 (Seven) years
Record of directors	Electronic and physical	7 (Seven) years
Minutes of directors' meetings	Electronic and physical	7 (Seven) years
Financial records of the Company		
Annual financial statements	Electronic and physical	7 (Seven) years
Accounting records as required by the Companies Act 71 of 2008	Electronic and physical	7 (Seven) years
Financial agreements	Electronic and physical	7 (Seven) years
Banking details	Electronic and	7 (Seven) years

	physical	
South African Reserve Bank (“SARS”) submissions and other documents relating to taxation	Electronic and physical	5 (Five) years after submission to SARS
Insurance of the Company		
Insurance policies held by the Company	Electronic and physical	7 (Seven) years
Register of all immovable property owned by the Company	Electronic and physical	7 (Seven) years
Employees		
List of Employees	Electronic and physical	3 (Three) years
Personal information of employees	Electronic and physical	3 (Three) years after termination
Employee contracts of employment	Electronic and physical	3 (Three) years after termination
Pension fund and provident fund	Electronic and physical	3 (Three) years
Salaries of employees	Electronic and physical	3 (Three) years
Leave records	Electronic and physical	3 (Three) years
Health and safety – records of earnings and other prescribed particulars of all employees	Electronic and physical	4 (Four) years
Health and Safety – committee and incident reports	Electronic and physical	3 (Three) years
Company policies and directives		
Internal policies, procedures and directives relating to employees and the company	Electronic and physical	7 (Seven) years
External policies, procedures and directives relating to clients and other third parties	Electronic and physical	7 (Seven) years
Agreements or contracts		
Standard agreements	Electronic and physical	3 (Three) years after termination
Contracts concluded with customers	Electronic and physical	5 (Five) years after termination

Non-disclosure agreements	Electronic and physical	3 (Three) years after termination
Letters of intent, memoranda of understanding	Electronic and physical	3 (Three) years after termination
Third party contracts (such as joint venture agreements)	Electronic and physical	3 (Three) years after termination
Office management contracts	Electronic and physical	3 (Three) years after termination
Supplier contracts	Electronic and physical	3 (Three) years after termination
Regulatory		
Licenses or authorities	Electronic and physical	Indefinite
Published Information		
External newsletters and circulars	Electronic and physical	1 (One) year
Internal newsletters and circulars	Electronic and physical	1 (One) year
Information on the Company published by third parties	Electronic and physical	1 (One) year
Customer Information		
Customer details	Electronic and physical	5 (Five) years after termination
Contact details of individuals within customers	Electronic and physical	5 (Five) years after termination
Communications with customers	Electronic and physical	3 (Three) years after termination

WEBSITE PRIVACY POLICY

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. COMMITMENT TO YOUR PRIVACY

2.1. Welcome to the website set out in item 1.6 of the Schedule (" **Website**"), owned and operated by the Company set out in item 1.1 of the Schedule ("**Company**"). The Company is committed to protecting the privacy of the user of the website. The Company values the trust of its subscribers and all others who work with it, and the Company recognises that maintaining your trust requires transparency and accountability in how the Company handles your Personal Information. This privacy policy ("**Policy**") is incorporated into and is subject to the Company's standard terms and conditions and the general terms relating to the use of the Website.

2.2. In performing the Company's services in the ordinary course of business, the Company may collect, use and disclose Personal Information. Anyone from whom the Company collects such information can expect that it will be appropriately and lawfully protected and that any use of or other dealing with this information is subject to consent, where this is required by law. This is in line with the general privacy practices of the Company.

2.3. This Policy sets out how the Company collects, uses, discloses, and safeguards the Personal Information it processes in the course of its business.

3. DEFINITIONS

3.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Company makes use of the following terms:

3.1.1. "**Personal Information**" means all information which may be considered to be personal in nature or information about an identifiable natural and / or existing juristic person (where applicable) in terms of the Electronic Communications and Transactions Act 25 of 2002 ("**ECTA**"), the Consumer Protection Act 68 of 2008 ("**CPA**") and the Protection of Personal Information Act 4 of 2013 ("**POPIA**"); and

3.1.2. "**User, you, your or yourself**" refers to any person who makes use of the Website for any purposes whatsoever, whether or not such use is free of charge or paid for.

3.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

4. WHAT PERSONAL INFORMATION DOES THE COMPANY COLLECT AND WHY?

The Company may collect Personal Information in conducting its ordinary business operations, including through the use of its Website. In processing such Personal Information, the Company at all times ensures that (i) it complies with the provisions of POPIA, and (ii) such Personal Information is used for legitimate business purposes.

5. OBTAINING CONSENT

The Company does not, except where otherwise permitted by law, collect, use or disclose your Personal Information without your consent.

6. USE AND DISCLOSURE OF PERSONAL INFORMATION

6.1. The Company operates its Website, and conducts its business in general, in accordance with South African legislation. The Company considers it imperative to protect the privacy interests of data subjects.

6.2. In the event that the Company sends Personal Information outside of South Africa (including if such information is hosted offshore), the Company will ensure that it takes all reasonable steps to ensure that it complies with all applicable laws in this regard, including POPIA.

7. RETENTION OF PERSONAL INFORMATION

All Personal Information retained on the Company's database, including such information obtained through the use of the Website, is in accordance with the retention provisions set out in the applicable laws and regulations of South Africa, including those set out in POPIA

8. YOUR RIGHTS IN RELATION TO YOUR PERSONAL INFORMATION

8.1. It is important to note that you have rights in relation to your Personal Information.

8.2. You have the right to contact the Company at any time to ask the Company to:

8.2.1. confirm that it holds your Personal Information (at no charge);

8.2.2. provide you access to any records containing your Personal Information or a description of the Personal Information that the Company hold about you (subject to payment of a prescribed fee); and / or

8.2.3. confirm the identity or categories of third parties who have had, or currently have, access to your Personal Information (also subject to payment of a prescribed fee).

8.3. The Company's contact information is as set out in item 1.1 of the Schedule.

8.4. When you make a request regarding your Personal Information, the Company will take reasonable steps to confirm your identity.

8.5. There may be times when the Company cannot grant access to your Personal Information, including where granting you access would (i) interfere with the privacy of others, or (ii) result in a breach of confidentiality. The Company will always provide you with reasons if this is the case.

8.6. If you are of the view that any Personal Information that the Company holds about you is incorrect in any way, including that it is inaccurate, irrelevant, outdated, incomplete or misleading, you are allowed to ask the Company to correct it. If you believe that any Personal Information that the Company holds about you is excessive or has been unlawfully obtained, you can ask the Company to destroy or delete it. You may do the same if you think that the Company has retained if for longer than necessary, given the purpose. The Company will do so unless there are good grounds not to (such as that the Company is required to hold it for a period prescribed by any applicable legislation).

8.7. It is important, however, to understand that if you withdraw your consent for the Company to use some of your Personal Information, it may affect the quality and level of service that the Company can provide to you.

9. SECURITY

9.1. The Company has adopted a security model to protect your Personal Information that complies with generally accepted information security practices and procedures. As part of the Company's security systems, the Company has implemented fire-wall technology, password controls, encryption processes and antivirus software. This is in addition to as the physical security measures adopted by the Company to ensure that it takes all appropriate, reasonable technical and organisational measures to prevent (i) loss of, damage to, or unauthorised destruction of Personal Information, and (ii) unlawful access to or processing of Personal Information. The Company has a stringent security policy in place that every officer, employer and supplier of the Company must adhere to.

9.2. The Company confirms that it takes all reasonable measures to:

9.2.1. identify all reasonably foreseeable internal and external risks to any Personal Information in its possession or under its control;

9.2.2. establish and maintain appropriate safeguards against any risks that are identified by the Company;

9.2.3. regularly verify that these safeguards are effectively implemented by or on behalf of the Company; and

9.2.4. ensure that such safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

10. COOKIES

10.1. The Website uses cookies in a limited way.

10.2. Cookies are small files containing information that a website uses to track a visit by a user. The Company uses session cookies to better understand how the Website is used by users to improve the performance of the Website for users, particularly the way search pages are delivered. The Company has installed settings on the Website to ensure that session cookies do not remain on your computer at the end of your visit to the Website, and cannot be used to obtain any personally identifiable details.

11. THIRD-PARTY WEBSITES

11.1. The Website may contain links to third party websites. In the event that you follow a link to any of these websites, it is important to note that these websites have their own terms of use and privacy policies and that the Company does not accept any responsibility or liability for them. If you (i) are a client of the Company, or (ii) are a user of the Website, and you have purchased products or services from the Company, the Company may use your contact details to send you details of any new similar products or services which the Company thinks you would be interested in. In doing so, the Company will at all times comply with any applicable direct marketing laws.

11.2. Any communications that you do receive from the Company pursuant to clause 11.1 will set out how to opt out of receiving future communications from the Company, free of charge, if you no longer wish to receive material for any reason whatsoever. The Company will only send you marketing messages when you tick the relevant boxes at certain times when engaging with the Company.

11.3. As the Company is not responsible for any representations, information, warranties and / or content on any website of any third party (including websites linked to this Website), the Company does not exercise control over third parties' privacy policies and the onus is on the User to refer to the privacy policy of any such third party before providing them with any of your Personal Information.

12. UPDATING OF PRIVACY POLICY

The Company, in its sole discretion, reserves the right to update, modify or amend this Policy from time to time with or without notice. You therefore agree and undertake to review the Policy whenever you visit the Website. Save as expressly provided to the contrary in this Policy, any amended version of the Policy shall supersede and replace all previous versions thereof.

13. CONTACT INFORMATION

Questions, concerns or complaints related to this Policy or the Company's treatment of Personal Information should be directed to the email address set out in item 1.5 of the Schedule.

Handling and Processing of Requests from Data Subjects in relation to POPIA

1. SCHEDULE
2. INTRODUCTION
3. OBJECTIVE
4. SCOPE
5. REREFENCE DOCUMENTS
6. PROCEDURES
7. RIGHTS RESERVED BY THE COMPANY
8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
9. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

2.1. All of the sections of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") became effective on 1 July 2020. In terms of POPIA, all data subjects, as this term is defined in POPIA ("**Data Subject/s**") have the right to request an organisation to confirm whether such organisation holds information about them.

2.2. For this reason, the company set out in item 1.1 of the Schedule ("**Company**") has implemented this policy ("**Policy**") to regulate any requests by Data Subjects for any personal information, as this term is defined in POPIA ("**Personal Information**"), that the Company may process in relation to such Data Subject.

2.3. At the outset, it must be understood that no information will be provided by the Company unless (i) the Data Subject has requested this in writing, (ii) the Data Subject has been properly identified, and (iii) all other provisions set out in this Policy have been complied with.

3. OBJECTIVE

The objective of this procedure is to effectively assist Data Subjects that approach the Company so that the Company can provide the Data Subject in question with a record or a description of their Personal Information that the Company may store on its systems.

4. SCOPE

4.1. This document is applicable to all Data Subjects that have the right to request a record or description of their Personal Information held by the Company.

4.2. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in POPIA, such terms will be given the meaning ascribed to them in POPIA.

5. REREFENCE DOCUMENTS

This policy should be read in conjunction with any other of the Company's privacy policies that may be relevant including, without limitation, the Information Privacy Policy of the Company.

6. PROCEDURES

6.1. **Formal request from the Data Subject**

6.1.1. A formal request from a Data Subject for information that the Company holds about them, must be made in writing accompanied with adequate proof of identification, which at a minimum includes a certified copy of the Data Subject's (i) identity document ("**ID**") or passport, and (ii) proof of residence.

6.1.2. Any (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("**Users**") who receive a written request in respect of data held by the Company in relation to POPIA must forward it to the information officer of the Company ("**Information Officer**") immediately. A Data Subject has a right to request this information.

6.2. **Processing the request from the Data Subject**

6.2.1. **Natural Person Data Subject requesting information**

6.2.1.1. The natural person Data Subject must request in writing (i) whether the Company processes any of their Personal Information, and (ii) a record of such Personal Information. This written request must be sent to the Information Officer. The Information Officer will request a certified copy of the individual's (i) ID or passport, and (ii) proof of residence. Once

this has been received and verified, the Information Officer will then be authorised to release the Personal Information in question (unless the Company cannot release such information for good reason, such as if granting the Data Subject access would interfere with the privacy of others or would result in a breach of confidentiality by the Company. The Company will always provide the Data Subject with written reasons if this is the case.

6.2.1.2. The Information Officer must:

6.2.1.2.1. record the Data Subject request on the Company's request system; and

6.2.1.2.2. safely store the certified copy of the (i) ID and passport, and (ii) proof of address, either in a file in a locked cupboard (if these are in paper format) or online in an encrypted folder which cannot be accessed by an unauthorised party.

6.2.2. **Juristic Person requesting information**

6.2.2.1. The Juristic person in question must request in writing (i) whether the Company processes any of its Personal Information, and (ii) a record of such Personal Information. This written request must be sent to the Information Officer. The Information Officer must then request an appropriate document to identify such Juristic person. For a company this will be certified copies of the following:

6.2.2.1.1. CIPC documents;

6.2.2.1.2. FICA documents for the company (including proof of business premises); and

6.2.2.1.3. Directors details and copies of all director's ID's or passports.

6.2.2.2. Once such documents have been received, the Information Officer will then be authorised to release the personal information to the individual (unless the Company cannot release such information for good reason, such as if granting the Data Subject access would interfere with the privacy of others or would result in a breach of confidentiality by the Company. The Company will always provide the Data Subject with written reasons if this is the case). The Information Officer must:

6.2.2.2.1. record the Data Subject request on the Company's request system; and

6.2.2.2.2. safely store the certified copies of all of the above documents either in a file in a locked cupboard (if these are in paper format) or online in an encrypted folder which cannot be accessed by an unauthorised party.

6.3. **Update the information of the Data Subject**

6.3.1. The Data Subject may request the Company to (i) correct or delete and of his / her / its Personal Information if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or has been obtained unlawfully, or (ii) destroy such record of Personal Information. If such a request is made, the Company must send this request to the Information Officer, who will then decide what action to take in respect of such Personal Information. If the information is destroyed or deleted, the Data Subject must be provided with credible evidence that this has been done. If instructed to do so by the Information Officer, the User in question must advise the Data Subject of any adverse consequences of deleting of destroying any Personal Information, including whether this will have an impact on the Company's ability to provide goods and / or services to the Data Subject, if this is applicable in the circumstances.

6.4. **Timeline**

6.4.1. As soon as a request for information has been received in writing and the Data Subject has been properly identified and verified, the Company will have 20 (Twenty) working days to provide the Data Subject with the information in question, subject to anything to the contrary set out in this Policy.

6.5. **Cost of providing information**

6.5.1. Data Subjects have the right to contact the Company to ask the Company to:

6.5.1.1. confirm that the Company holds the Data Subject's Personal Information at no charge;

6.5.1.2. provide the Data Subject with access to any records containing the Data Subject's Personal Information or a description of such Personal Information that the Company holds, subject to payment of a prescribed fee under POPIA; and / or

6.5.1.3. confirm the identity or categories of third parties who have had, or currently have, access to the Data Subject's Personal Information, also subject to payment of a prescribed fee under POPIA.

6.6. **Delivery method of the information**

6.6.1. Information may be shared with the Data Subject under this Policy in the following ways:

6.6.1.1. The information may be provided to the Data Subject in person; provided that the Data Subject must sign for the information received; or

6.6.1.2. The information may be provided to the Data Subject to the email address that such Data Subject has chosen in writing. Any information provided by email must be password protected with an 8 (Eight) character password that must contain at least one upper case and lower case character, and at least one numeric and one special character; provided that the password:

6.6.1.2.1. must not be sent in the same email as the information; and

6.6.1.2.2. must be sent via a different application, preferably WhatsApp. This will prevent an unauthorised individual having access to the email address being able to open the file without also having the password.

7. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

9. POLICY AWARENESS AND UPDATE

9.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

9.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

9.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Information Incident Management Policy and Process

1. SCHEDULE
2. INTRODUCTION
3. PURPOSE
4. SCOPE
5. SUPPORTING DOCUMENTS
6. POLICY
7. INFORMATION INCIDENTS
8. RIGHTS RESERVED BY THE COMPANY
9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS
10. POLICY AWARENESS AND UPDATE

1. SCHEDULE

1.1	The Company : Groot Constantia Trust NPC RF	
1.2	Registration number : 1993/003391/08	
1.3	VAT registration number : 4030108080	
1.4	Physical address	
	Groot Constantia Estate, Groot Constantia Road, Constantia,7806	
1.5	Email address : ceo@grootconstantia.co.za	

2. INTRODUCTION

This policy ("**Policy**") was developed to provide direction to guide all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the systems ("**Users**") of the Company set out in item 1.1 ("**Company**") on how to respond to incidents that threaten the security of personal information, as this term is defined in the Protection of Personal Information Act 4 of 2013, and other relevant privacy legislation such as the General Data Protection Regulation, where this may be applicable ("**Personal Information**").

3. PURPOSE

3.1. The purpose of this Policy is to:

3.1.1. provide a policy framework for responding to information incidents (including data breaches) in accordance with the relevant privacy legislation referred to above; and

3.1.2. assist the Users in understanding their responsibilities in addressing and dealing with Information Incidents.

4. SCOPE

4.1. This Policy applies to (i) all Users, and / or (ii) any person handling information or data processed by the Company.

4.2. Unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

5. SUPPORTING DOCUMENTS

This Policy should be read in conjunction with other policies of the Company that regulate the protection of Personal Information.

6. POLICY

The incident management of an information incident is vital to the Company. By handling such incidents efficiently and correctly, the impact on the reputation of the Company, and other damage to the Company can be managed. Implementing the necessary control measures in the case of an information or data breach is critical.

7. INFORMATION INCIDENTS

7.1. This section of the Policy sets out the steps that must be taken in response to an Information Incident within, or in relation to, the Company, including the roles and responsibilities of all stakeholders involved.

7.2. An "**Information Incident**" means a single or a series of unwanted or unexpected events that threaten information security or privacy. Information Incidents include any collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorised by the Company or the owner of such information.

7.3. Information Incidents include "Privacy Breach/es", which are unauthorised collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alteration, consultation, use or dissemination by means of transmission, merging, linking, disposal (erasure or destruction), or storage of Personal Information, whether accidental or deliberate. If these breaches include Personal Information, POPIA will be applicable to both Information Incidents and Privacy Breaches.

7.4. **Incident Committee**

7.4.1. The incident committee ("**Committee**") is responsible for the coordination, investigation, and resolution of all Information Incidents in association with the information officer of the Company ("**Information Officer**").

7.4.2. The Committee will comprise of a selection of management representatives of the Company.
7.4.3. The Committee will be responsible for determining when a decision must be made to either notify or not notify data subjects of an Information Incident based on a balance of harms or, where applicable, as required by relevant legislation, including POPIA.
7.4.4. The Information Officer is solely responsible for liaising with the information regulator ("**Regulator**") regarding an actual or suspected Privacy Breach. The only exception to this is in the case of a whistle blower employee of the Company who shares information with the Regulator in good faith.

7.5. **Process: Information Incident reporting**

7.5.1. Any User or other person who discovers a suspected or actual Information Incident, including a Privacy Breach, must immediately report it to their supervisor and or manager. The supervisor or manager must then report it to the Information Officer immediately. The Information Incident must then be recorded in an incident register ("**Register**").
7.5.2. In circumstances where the supervisor or management contact is not immediately available, whether in person or by phone, the User must immediately report the Information Incident directly to the Information Officer.
7.5.3. Where the Information Incident will have serious impact on the Company, the Information Officer must contact the person reporting the Information Incident to:
7.5.3.1. assess and document the Information Incident including, if applicable, the nature, sensitivity, volume, impact and type of incident in question;
7.5.3.2. assist with resolving the Information Incident and containing the Information Incident if it has not yet been fully resolved; and
7.5.3.3. provide the person reporting the Information Incident with instructions regarding how to deal with the Information Incident response process and priorities, such as (i) containing the loss, (ii) preventing a recurrence and (iii) determining the next steps.
7.5.4. The Information Officer must decide if additional information should be gathered to determine the response strategy to the Information Incident and to define work assignments according to various relevant factors, including the:
7.5.4.1. type of Information Incident;
7.5.4.2. nature and sensitivity of the Information Incident;
7.5.4.3. volume; and
7.5.4.4. impact and implications of unauthorised disclosures or asset losses.
7.5.5. The Information Officer determines whether the Information Incident is major or minor, based on relevant factors that include the following:
7.5.5.1. The Information Incident involves (i) Personal Information, and / or (ii) sensitive, confidential, proprietary and / or critical information of the Company ("**Confidential Information**");
7.5.5.2. Whether there is, or could have been, a reasonable expectation of harm to any data subject as a result of the Information Incident;
7.5.5.3. Whether data subjects will be, or have been, notified that their Personal Information has been compromised;
7.5.5.4. Whether the incident will be, or has been, reported to the Committee; and / or
7.5.5.5. Whether the Information Incident has a serious or potentially serious public impact.
7.5.6. Minor Information Incidents:
7.5.6.1. The information asset owner in question ("**IAO**") will be the main point of contact for the breach in question;
7.5.6.2. The IAO will refer all minor Information Incidents to the Information Officer for follow-up and resolution in collaboration with chief executive officer of the Company ("**CEO**"); and
7.5.6.3. The Information Officer must request the IAO to provide a report regarding the Information Incident.
7.5.7. Major Information Incidents:
7.5.7.1. The IAO must coordinate an incident management and investigation process in order to conduct an assessment and gather evidence regarding the Information Incident; and
7.5.7.2. Status reports must be sent to the Information Officer who in turn will provide periodic updates to the Committee where appropriate.
7.5.8. Where the root cause of the Information Incident has a major adverse impact on the Company, change management must be initiated.

7.6. **Notification of the Regulator**

7.6.1. The Committee, in conjunction with the Information Officer, will determine if there was a breach of any data subject's Personal Information, and whether such breach should be reported to the Regulator. The following factors need to be taken into account before reporting any Information Incident to the Regulator:
7.6.1.1. The nature of the Information Incident in question;
7.6.1.2. The legitimate needs of, and requirement for, law enforcement to act on the Information Incident;
7.6.1.3. Measures that are reasonably necessary to determine the scope and extent of the compromise in question; and
7.6.1.4. Measures that should be taken to restore the integrity of the Company's information systems.
7.6.2. The Information Officer must ensure that any breach or compromise is reported to the Regulator as soon as reasonably possible after the discovery of the compromise as required by Section 22 of POPIA, and once the factors set out in clause 7.6.1 have been considered.

7.7. **Notification of affected individual data subjects**

7.7.1. The impact of Privacy Breaches must be reviewed to determine if it is appropriate to notify individual data subjects whose Personal Information has been affected by the breach in question. The IAO will work with the Information Officer to notify affected parties and take other required action that may be appropriate in the circumstances.
7.7.2. The key consideration in deciding whether to notify an affected individual is whether such notification is necessary in order to avoid or mitigate harm to an individual, such as a risk:
7.7.2.1. identity theft or fraud;
7.7.2.2. of physical harm;
7.7.2.3. of damage to reputation; and / or

7.7.2.4. to business or employment opportunities.

7.7.3. Other considerations in determining whether to notify individual data subjects include the following:

7.7.3.1. Any legislative requirements for notification such as required by Section 22 of POPIA;

7.7.3.2. Any contractual obligations that may require notification; and / or

7.7.3.3. A risk of loss of confidence in the Company and / or good customer / client relations dictate that notification is appropriate.

7.7.4. Notification is determined based on the balance of harms. Under this principle, an individual data subject who could potentially face harm as a result of an Information Incident may not be notified if it is determined that the harm that would result from a notification would outweigh the benefit to be gained from the notification.

7.7.5. Where an Information Incident involves the potential for significant harm to an individual data subject, any decision not to notify such an individual must be approved jointly by the Information Officer and the Committee.

7.7.6. If it is determined that notification of individual data subjects would be appropriate in the circumstances of any Information Incident, the:

7.7.6.1. notification should occur as soon as possible following the breach in question; and

7.7.6.2. all affected individuals should be notified directly, whenever possible.

7.8. **Closure of Information Incident file**

7.8.1. When closing an Information Incident file, the Information Officer must notify the IAO and the Committee. The Information Officer will also write a final report ("**Report**"), including recommendations, and submit it to all stakeholders. There are 2 (Two) types of recommendations included in the Report, namely:

7.8.1.1. essential recommendations, which must be implemented promptly; and

7.8.1.2. advisory recommendations, which the CEO will decide whether or not to implement, informing the Information Officer and the Committee of his / her decision.

7.9. **Compliance**

7.9.1. The CEO and / or the Information Officer, as applicable, will be responsible for implementing the recommendations set out in the Report and reporting the status of such recommendation.

7.9.2. The Information Officer will present the recommendations set out in the Report, and the results of implementing such recommendations to the Committee.

7.9.3. The Information Officer may perform compliance reviews or may audit the implementation of the recommendations set out in the Report and their effectiveness once implemented.

7.10. **Responsibilities**

7.10.1. **User**: In the case of any actual or suspected Information Incident, the User's responsibilities are to:

7.10.1.1. report the Information Incident immediately to the Information Officer, the IAO and / or their supervisor / manager;

7.10.1.2. recover the (i) Personal Information, and / or (ii) Confidential Information if possible, or to otherwise contain the Information Incident so as to lessen its impact and implication for the Company and the data subjects involved; provided that if the Information Incident involves any information technology ("**IT**"), the direction of the chief information officer ("**CIO**") must be sought before any containment steps are taken;

7.10.1.3. remediate the Information Incident by working collaboratively with the IAO and Information Officer to determine the specifics of the Information Incident in order to resolve it; and

7.10.1.4. prevent Information Incidents by being diligent in the handling of (i) Personal Information, and / or (ii) Confidential Information, and being an active participant in developing the culture of prudent information management within, or in relation to, the Company.

7.10.2. **IAOs**: In the case of the actual or suspected Information Incident, the IAO's responsibilities are to:

7.10.2.1. receive the report about the Information Incident from the User and provide direction on assessing the Information Incident and ensuring its recordal in the Register;

7.10.2.2. determine if the (i) Personal Information, and / or (ii) Confidential Information in question can be recovered, or if the loss / disclosure can otherwise be contained; provided that if the Information Incident involves any IT, the direction of the CIO must be sought before any containment steps are taken;

7.10.2.3. work collaboratively with the Information Officer to determine the specifics of the Information Incident and to implement the steps needed to resolve it;

7.10.2.4. prevent Information Incidents by:

7.10.2.4.1. implementing the recommendations set out in the Report and ensuring that Users know and understand how to apply changes in the handling of (i) Personal Information, and / or (ii) Confidential Information;

7.10.2.4.2. participating in the development of a culture within, or in relation to, the Company for the prudent management of information, including by providing appropriate training;

7.10.2.4.3. ensuring that Users understand their responsibility in reporting all actual and suspected Information Incidents, including the importance of containing the loss and / or recovering the information in question;

7.10.2.4.4. notifying any data subjects (both individuals and juristic entities) affected by the Information Incident, where directed to do so; and

7.10.2.4.5. ensuring that contractors and other service providers understand their responsibilities in the Information Incident reporting process and collaborating with them to ensure timely and accurate reporting.

7.10.3. **Contractor or service provider**: Where the User in question is a contractor or other service provider ("**Contractor/s**"), in the case of an actual or suspected Information Incident, the Contractor's responsibilities are to:

7.10.3.1. ensure that any of their employees, service providers, or any other persons who discover a suspected or actual Information Incident (including a Privacy Breach) immediately notify the management of such Contractor, who must then report it to the contract manager at the Company, the Information Officer and / or CEO;

7.10.3.2. ensure that the Information Incident is immediately recorded in the Register and that the Committee is notified;

7.10.3.3. recover the (i) Personal Information, and / or Confidential Information if possible, or to otherwise contain the incident to lessen the impact and implication for the Company and any data subjects involved; provided that if the Information Incident

involves any IT, the direction of the CIO of the Contractor must be sought before any containment steps are taken by the Contractor;

7.10.3.4. remediate the Information Incident:

7.10.3.4.1. with the Company's contract manager as the initial owner of the Information Incident;

7.10.3.4.2. by working collaboratively with the contract manager in question and the Information Officer;

7.10.3.4.3. by supporting the investigation and Information Officer, or any others to determine the specifics of the Information Incident in order to resolve it; and

7.10.3.4.4. by notifying any data subjects (whether individuals or juristic persons) affected by the Information Incident, where and as directed by the Information Officer and the contract manager in question;

7.10.3.5. prevent Information Incidents by:

7.10.3.5.1. ensuring that employees know and understand how to apply changes in the handling of (i) Personal Information, and / or Confidential Information;

7.10.3.5.2. being diligent in the handling of (i) Personal Information, and / or (ii) Confidential Information;

7.10.3.5.3. implementing recommendations from the Information Incident reporting process and reporting the results to the Information Officer;

7.10.3.5.4. developing a culture for the prudent management of information within the Contractor's business, including by providing training; and

7.10.3.5.5. ensuring that their employees understand their responsibility in reporting Information Incidents, including containing the loss and / or recovering the information in question.

7.10.4. **The Information Officer**: The Information Officer's responsibilities in respect of any suspected or actual Information Incident is to:

7.10.4.1. be for the coordination, investigation, and resolution of all Information Incidents, including Privacy Breaches;

7.10.4.2. receive and review status reports and, where applicable, compile the Report and present to the Committee and / or CEO on the implementation of the recommendations contained in the Report;

7.10.4.3. ensure that the recommended controls in the Report are appropriately implemented through effective audits;

7.10.4.4. Report Information Incidents to the Committee;

7.10.4.5. contact all responsible stakeholders to ensure appropriate communication, recommendation, and collaboration, where appropriate; and

7.10.4.6. liaise with the Regulator on Privacy Breaches and other Information Incidents, where appropriate.

8. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the aforegoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

10. POLICY AWARENESS AND UPDATE

10.1. **Training and awareness**: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

10.2. **Dissemination**: This Policy will be made available on the Company's network, intranet or similar portals.

10.3. **Review**: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.