PROTECTION OF PERSONAL INFORMATION POLICY

TABLE OF CONTENTS

1. **INTRODUCTION**

1.1 Whereas the Organisation is obliged to comply with POPI.

1.2 The Organisation is required to inform all Persons as to how their Personal Information is used, disclosed and destroyed.

1.3 The Organisation is committed to protecting a Person's privacy and ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

1.4 Wherefore this Policy sets out a manner in which the Organisation deals with Personal Information as well as stipulates the purposes for which said information is used. This Policy must also be read with the Information Management Policy as well as the Information Technology and Electronic Communications Policy.

2. **DEFINITIONS AND INTERPRETATION**

2.1. Unless otherwise expressly stated, or the context otherwise requires, the words and expressions listed below shall, when used in this Policy bear the meanings ascribed to them below and cognate expressions bear corresponding meanings:

2.1.1. "Board" means the Board of Directors of the Organisation serving from time to time;

2.1.2. “Child” means a natural person under the age of 18 years who is not legally competent, without the assistance of a Competent Person, to take any action or decision in respect of any matter concerning him or herself;

2.1.3. “Competent Person” means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

2.1.4. “Consent” means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

2.1.5. “Data Subject” means the person to whom personal information relates;

2.1.6. “Directors” means those persons appointed as executive or non-executive directors to the Board according to the Organisation’s Memorandum of Incorporation and the ruling policies and procedures applicable to the Organisation from time to time;

2.1.7. “Disaster Project Team” means the Group COO, Finance Manager and the Production Manager of the Organisation;

2.1.8. Electronic communication” means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

2.1.9. “Employee” means an Employee of the Organisation;

2.1.10. “Filing System” means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

2.1.11. “GDPR” means the General Data Protection Regulation;

2.1.12. “Information Officer” means a Director or Manager of the Organisation who is tasked with being the Information Officer;

2.1.13. “Information Regulator” means the information regulatory body established under section 39 of POPI contactable at:
Email: inforeg@justice.gov.za / Tel: 012 406 4818 / Fax: 086 500 3351.

2.1.14. “IT equipment” means computers, laptops, mobile phones and other electronic devices;

2.1.15. “Level of Risk” means the magnitude of a risk expressed in terms of the combination of consequences and their likelihood;

2.1.16. “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;

2.1.17. “Organisation” means Earth Touch (Pty) Ltd with registration number 2006/014191/07;

2.1.18. “Other Confidential Information” means confidential information relating to the Organisation, including but not limited to: trade secrets, confidential information (i.e. information that is not known in public), technical know-how and data, drawings, system, methods, software processes, client lists, programs, marketing and/or financial information except where such information must be shared between the Organisation and an Employee or between Employees for the purpose of employment or association with the Organisation;

2.1.19. “Person” means a natural person and may include a customer, franchisee, vendor, independent contractor, job applicants and Employees;

2.1.20. “Personal Information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-

2.1.20.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

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

2.1.20.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.1.20.4. the biometric information of the person;

2.1.20.5. the personal opinions, views or preferences of the person;

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

2.1.20.7. the views or opinions of another individual about the person; and

2.1.20.8. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

2.1.21. “POPI” means the Protection of Personal Information Act 4, 2013, as amended from time to time;

2.1.22. “Policy” means this POPI policy;

2.1.23. “Prescribed” means prescribed by regulation or by a code of conduct;

2.1.28. “Processing” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

2.1.28.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

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

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

2.1.24. “Public Record” means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

2.1.25. “Record” means any recorded information—

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

2.1.25.1.1. writing on any material;

2.1.25.1.2. information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

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

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

2.1.25.1.5. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

2.1.25.1.6. in the possession or under the control of a Responsible Party;

2.1.25.1.7. whether or not it was created by a Responsible Party; and

2.1.25.1.8. regardless of when it came into existence;

2.1.26. ‘‘Regulator’’ means the Information Regulator established in terms of section 39 of POPI;

2.1.27. “Responsible Party” means the person who determines what information is required and processes that information including where such person outsources part or all of the processing to an Operator;

2.1.28. “Risk Assessment” means the process to comprehend the nature of the risk and to determine the ‘Level of Risk’.

2.1.29. “Special Personal Information” means religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, in terms of section 26 of POPI.

2.2. In this Policy:

2.2.1. table of contents and paragraph headings are for purposes of reference only and shall not be used in interpretation;

2.2.2. unless the context clearly indicates a contrary intention, any word connoting any gender includes the other genders, and the singular includes the plural and vice versa;

2.2.3. When a number of days are prescribed such number shall exclude the first and include the last day unless the last day is not a business day, in which case the last day shall be the next succeeding business day.

3. PERSONAL INFORMATION TO BE COLLECTED

3.1. The Organisation collects the following personal information:

3.1.1. Personal Information of applicants for employment or internship with the Organisation for the purposes of confirming, verifying personal details, contacting, consideration, appointment and performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship where applicable as well as for legislative audit and record keeping purposes as well as compliance with legal and regulatory requirements (eg. Tax and labour law);

3.1.2. Personal Information of its contractors for the purposes of confirming, verifying and updating the Person's details, contracting in respect of transactions, audit and record keeping purposes;

3.1.3. Personal Information of its suppliers for the purposes of confirming, verifying and updating the Peron's details, contracting in respect of transactions, audit and record keeping purposes;

3.1.4. Personal Information that is necessary for compliance with a legal obligation to which the Organisation is subject;

3.1.5. Personal Information that is necessary for the purposes of the legitimate interests pursued by the Organisation or by a third party, except where such interests are overridden by the interests or fundamental rights and

freedoms of the Data Subject which require protection of Personal Information, in particular where the Data Subject is a child[1].

3.1.6. Any other Personal Information deemed necessary by the Organisation that complies with this Policy.

3.2. Personal information collected should be:

3.2.1. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

3.2.2. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

3.3. The above Personal Information, may also be used for any other reason as set out in paragraph 5 to this Policy.

3.4 We will only process your personal information for lawful purposes relating to our business if the following applies:

- if you have consented thereto.
- if a person legally authorised by you, the law, or a court, has consented thereto.
- if it is necessary to conclude or perform under a contract, we have with you.
- if the law requires or permits it.
- if it is required to protect or pursue your, our or a third party's legitimate interest.

4.Special Personal Information

4.1 When will we process your special personal information?

We may process your special personal information in the following circumstances:

- if you have consented to the processing.
- if the information is being used for any Human resource or payroll requirement.
- if the processing is needed to create, use, or protect a right or obligation in law.

[1] General Data Protection Regulations: Article 6 (Lawfulness of processing)

- if the processing is for statistical or research purposes and all legal conditions are met.

- if the special personal information was made public by you.

- if the processing is required by law.

- if racial information is processed, and the processing is required to identify you; and / or if health information is processed, and the processing is to determine your insurance risk, or to comply with an insurance policy or to enforce an insurance right or obligation.

4.2 When and from where we obtain personal information about you?

We may collect personal information about you from the following sources:

- We may collect personal information directly from you.

- We may collect personal information from a public record.

- We may collect personal information from an area where you have deliberately made it public.

- We may collect information about you based on your use of our products, services, or service channels.

- We may collect information about you based on how you engage or interact with us such as via our support desk, emails, letters, telephone calls and surveys.

- We may collect personal information from a third party.

- We may collect personal information from another source if you give us consent to do so.

If the law requires us to do so, we will ask for your consent before collecting personal information about you from third parties.

The third parties from whom we may collect your personal information include, but are not limited to, the following:

- Partners of our company for any of the purposes identified in this Privacy Policy.

- your spouse, dependents, partners, employer, and other similar sources.

- attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements.

- payment processing services providers, merchants, banks, and other persons that assist with the processing of your payment instructions, like EFT transaction partners.

- insurers, brokers, other financial institutions, or other organisations that assist with insurance and assurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims and other related purposes.

- law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime;

- regulatory authorities, industry ombudsman, governmental departments, local and international tax authorities.

- trustees, Executors or Curators appointed by a court of law.

- courts of law or tribunals.

4. HOW TO TREAT PERSONAL INFORMATION COLLECTED

4.1. *Accountability:*

4.1.1. Should the Organisation collect Personal Information, it is responsible for ensuring that the Personal Information is processed in accordance with the provisions of this Policy.

4.2. *Processing limitation:*

4.2.1. The Organisation must process the Personal Information of a Person in a lawful, fair and transparent manner.

4.2.2. The Organisation must obtain the consent of the Person prior to the disclosure of their Personal Information so as to not undermine the privacy of the Person.

4.2.3. Personal Information collected must be reasonable and for specified, explicit and legitimate purpose. It must further no be processed in a manner that is not consistent with the purpose for which it was intended.

4.2.4. A Person's Personal Information must be collected from the Person themselves and the Person must consent to the collection of their Personal Information by the Organisation.

4.2.5. A Person may withdraw their consent at any time.

4.2.6. The further processing of Personal Information must be compatible with the purpose for which it was originally collected.

4.3. *Purpose specification*

4.3.1. Personal Information must be collected for a specific purpose related to the business of the Organisation;

4.3.2. the Person must be aware of the purpose of the collection of their Personal Information. A Person must be able to decide whether or not they want to provide the Organisation with their Personal Information for that particular purpose; and

4.3.3. Personal Information must not be retained for longer that it may be required by the ruling regulatory framework or the Organisation 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 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by any law in order to safeguard the rights and freedoms of the Data Subject.

4.4. *Information quality*

4.4.1. The Organisation must take reasonable steps to ensure that the Personal Information collected is complete, accurate, not misleading and, where necessary, updated by the Organisation.

4.4.2. This shall ensure that the integrity of the Personal Information is maintained and ensure that the Personal Information remains accurate and reliable.

4.5. *Openness*

4.5.1. The Organisation must ensure that the Person is aware of the following:

i. that the Personal Information is being collected by the Organisation;
ii. the name and address of the Organisation;
iii. the purpose for which the Personal Information is collected;
iv. whether the disclosure of the Personal Information to the Organisation is voluntary or mandatory;
v. the consequences, if any, of a failure to provide the Personal Information;
vi. if the Personal Information will be transferred to a third party or outside of the RSA; and
vii. any other further and reasonable information.

4.6. *Data Subject participation*

4.6.1. A Person may request that the Organisation:

i. confirm whether the Organisation holds Personal Information about them;
ii. provide a description of the Personal Information held by the Organisation; and/or
iii. correct or delete their Personal Information.

4.7. *Records of processing activities*

4.7.1. The Information Officer shall maintain a record of processing activities under its responsibility and contain the information set out in article 30 of the GDPR.

4.8. *Confidentiality*

4.8.1. Anyone who processes information in terms of this Policy shall be subject to strict confidentiality and be expected to sign a confidentiality undertaking and/or agreement with the Organisation.

4.9. *Children*

The Personal Information of a childmay not be processed unless the processing is carried out with the prior consent of the child's parent or legal guardian.

5. THE USAGE OF PERSONAL INFORMATION

5.1. A Person's Personal Information will only be used for the purpose for which it was collected and agreed. This may include:

5.1.1. Providing products or services to the Person and to carry out the transactions requested;

5.1.2. Confirming, verifying and updating the Person's details;

5.1.3. For the detection and prevention of fraud, crime, money laundering or other malpractice;

5.1.4. Conducting market or customer satisfaction research;

5.1.5. For audit and record keeping purposes;

5.1.6. In connection with legal proceedings;

5.1.7. Providing services to Persons to carry out the services requested and to maintain and constantly improve the relationship;

5.1.8. In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

6. DISCLOSURE OF PERSONAL INFORMATION

6.1. The Organisation may share a Person's Personal Information with, and obtain information about Persons from third parties for the reasons already discussed above.

6.2. The Organisation may also disclose a Person's Personal Information where it has a duty or a right to disclose in terms of applicable legislation, the law or where it may be deemed necessary to protect its rights.

7. MARKETING

7.1 How we use your personal information for marketing

- We will use your personal information to market our products and services to you.
- We will do this in person, by post, telephone, or electronic channels such as SMS, email, and fax.
- If you are not our customer, or in any other instances where the law requires, we will only market to you by electronic communications with your consent.
- In all cases you can request us to stop sending marketing communications to you at any time.

8. TRANSBORDER INFORMATION FLOW

8.1 Under what circumstances will we transfer your information to other countries?

We will only transfer your personal information to third parties in another country in any one or more of the following circumstances:

- where your personal information will be adequately protected under the other country's laws or an agreement with the third-party recipient.
- where the transfer is necessary to enter into or perform under a contract with you, or a contract with a third party that is in your interest.
- where you have consented to the transfer; and / or
- where it is not reasonably practical to obtain your consent, the transfer is in your interest.

This transfer will happen within the requirements and safeguards of the law. Where possible, the party processing your personal information in the other country will agree to apply the same level of protection as available by law in your country or if the other country's laws provide better protection, the other country's laws would be agreed to and applied.

8. SAFEGUARDING PERSONAL INFORMATION

8.1. It is a requirement of POPI to adequately protect the Personal Information held by the Organisation and to avoid unauthorised access and use of Personal Information. The Organisation continuously reviews its security controls and processes to ensure that Personal Information is secure.

8.2. We will take appropriate and reasonable technical and organisational steps to protect your personal information according to industry best practices. Our security measures (including physical, technological, and procedural safeguards) will be appropriate and reasonable. This includes the following:

8.2.1 keeping our systems secure (like monitoring access and usage);

8.2.2 storing our records securely.

8.2.3 controlling the access to our buildings, systems and/or records; and

8.2.4 safely destroying or deleting records.

8.2.5 ensure compliance with best practice standards

8.3 The following procedures must be in place in order to protect Personal Information:

8.3.1 the Organisation's Information Officer whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of Personal Information and other provisions of POPI;

8.3.2 employees are required to sign Confidentiality Agreements which are considered annexures to their Employment Contracts, and receive induction on and a copy of this Policy;

8.3.3 hard copy files are securely stored in the filing room and electronic versions are stored on the server and are destroyed after 5 years of any contract or transaction mentioned in paragraph 3 to this Policy comes to an end;

8.3.4 the Organisation's internal server hard drives are protected and the Organisation also maintains a backup server remotely located to ensure the integrity and security of the information contained on the Organisation's Information Technology Infrastructure in the event of the loss or destruction of physical IT assets within the Organisation.

8.3.5 a disaster recovery register will be kept to log any security incidents and to report on and manage said incidents. This register will be maintained by the Information Officer.

8.3.6 consent to process a Person's Personal Information is obtained from the Person (or a person who is authorised by the Person to provide the candidates' Personal Information) during registration.

9 ACCESS AND CORRECTION OF PERSONAL INFORMATION

9.2 A Person has the right to access the Personal Information that the Organisation holds about them. A Person also has the right to ask for an update, correction or deletion their Personal Information on reasonable grounds. Once a Person objects to the processing of their Personal Information, the Organisation may no longer process such Person's Personal Information.

9.3 The Data Subject shall have the right to obtain from the Information Officer confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data[2].

[2] In terms of Article 15 of the General Data Protection Regulation, the Data Subject has the right to the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the

10 OTHER CONFIDENTIAL INFORMATION

10.2 Besides protecting Personal Information, the Organisation also has Other Confidential Information that must remain protected.

10.3 All Employees are to sign confidentiality agreements upon employment and induced and provided with a copy of this Policy as amended from time to time.

10.4 Users are entitled to access only those elements of IT Systems that are consistent with their authorisation

10.5 The data breach protocols in this Policy applies to Personal Information as well as Other Confidential Information.

11 RESPONSIBLE PARTY FOR PERSONAL AND OTHER CONFIDENTIAL DATA BREACHES

11.2 The Information Officer is responsible for managing personal and Other Confidential data security breaches in conjunction with the Board and the head of IT services within the Organisation.

11.3 In disaster situations, the Disaster Project Team shall take over responsibility and manage personal data security breaches in conjunction with the Information Officer.

Information Officer Details

Name	:	Lara Cox, Group COO
E-mail Address	:	lcox@earthtouchsa.com
Telephone Number (Tel: +44 7471798209		

12 REPORTING PERSONAL AND OTHER DATA BREACHES

12.2 In the event that an Employee becomes aware of an actual, potential or suspected breach of personal data security, the Employee must immediately report the incident to the Information Officer.

12.3 The Employee shall immediately or as soon as practicable, submit the attached Data Security Breach Form[3] to the Information Officer at lcox@earthtouchsa.com

12.4 All the relevant details of an incident are recorded consistently and communicated on a need-to-know basis to the relevant staff necessary to ensure prompt and appropriate action to resolve the incident.

13 MANAGING A PERSONAL OR OTHER CONFIDENTIAL DATA BREACH

13.2 The following five (5) steps must be followed systematically in responding to a personal data breach:

- Step 1: Identification & Initial Assessment
- Step 2: Containment & Recovery
- Step 3: Risk Assessment
- Step 4: Incident Report
- Step 5: Notification
- Step 6: Evaluation & Response

13.3 Step 1: Identification and initial assessment of the incident

13.3.1 Upon receipt of the Data Security Breach Form the Information Officer, shall conduct an initial assessment of the incident by establishing:

---

information as to their source; (h) the existence of automated decision-making.

a) if a personal data security breach has taken place;
b) what personal data is involved in the breach;
c) the cause of the breach;
d) the extent of the breach (how many individuals are affected);
e) the potential harm to affected individuals; and
f) measures to contain the breach.

13.3.2 The Information Officer shall determine the severity of the incident using the checklist contained in Appendix B and shall record this initial assessment in Part 2 of the Data Security Breach Form.

13.3.3 The severity of the incident will be categorised as level 1 (Local), 2a (Minor), 2b (Major) or 3 (Catastrophic).

13.3.4 Incidents shall be managed according to their severity. Levels 2b and 3 shall be escalated to the Disaster Project Team which will be responsible for the management and close-out of the incident. The Disaster Project Team is to manage the breach in conjunction with the Information Officer.

13.3.5 The Information Officer shall be responsible for the management and close-out of level 1 and 2a incidents. The Information Officer may if necessary, appoint a group of relevant stakeholders within the Organisation to assist with further investigation of such incidents.

13.4 Step 2: Containment and recovery

13.4.1 The Organisation must take immediate and appropriate steps to limit the identified data breach.

13.4.2 The Information Officer and Board shall establish:

a) Who within the Organisation needs to be made aware of the breach (Legal, IT, Public Relations etc).

b) What such persons are expected to do in order to contain the breach.

**this may include changing passwords, closing a compromised section of the network, finding lost equipment, contracting external experts.*

c) Whether measures can be taken to limit the damage caused by the breach.

**this may include the use of backups.*

d) Whether circumstances dictate that affected individuals are to be notified immediately (where there is a high level of risk of serious harm to affected individuals).

e) Whether it is appropriate to inform the South African Police Services

**in cases involving theft or other criminal activity.*

13.5 Step 3: Risk Assessment

13.5.1 Assessment of risk arising from a personal or Other Confidential data security breach is to be conducted by likelihood of consequences and the severity thereof.[4]

13.5.2 In assessing a risk arising from a personal data security breach, the Information Officer shall consider, in consultation with relevant stakeholders, the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. In this regard, Part 1 of the Data Security Breach Report Form shall be of assistance.

13.5.3 Risks to be assessed include, but are not limited to:

[4] This method is in accordance with the **GDPR Article 29 - Working party guidelines**; read with paragraph 4.5.3 ISO/IEC 27000:2018; the systematic approach of estimating the magnitude of risks (risk analysis); the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

a) Risks for the individuals affected:

- What are the potential consequences for individuals?
- How serious are these potential consequences?
- What is the likelihood of these consequences manifesting?

b) Risks for the Organisation

- Legal compliance.
- Financial.
- Reputational.
- Continuity of service delivery.

13.6 Step 4: Incident report

13.6.1 Following the risk assessment, and irrespective of the level of risk, the Information Officer must compile an Incident Report detailing:

a) A summary of the breach;
b) If known, Employees and other persons involved in or responsible for the breach;
c) Any details in respect of information, IT equipment or systems involved, lost or compromised in the breach;
d) Details as to how the breach occurred;
e) Actions taken and proposed to resolve the breach and the consequences flowing therefrom;
f) Potential consequences yet to materialise; and
g) Recommendations to prevent the reoccurrence of the breach.

13.6.2 A copy of the Incident Report shall be furnished to the Board.

13.7 Step 5: Notification

13.7.1 On the basis of the above risk assessment, the Board shall determine whether it is necessary to formally notify:

a) the Information Regulator;
b) individuals affected by the breach;
c) insurers of the Organisation;
d) SAPS;
e) financial institutions (banks, medical aid etc.)
f) press/media; and
g) external legal advisors

13.7.2 Notification to the Information Regulator and affected individuals, where necessary, should occur within 72 hours of the Organisation having reasonable certainty that a security incident occurred and personal data was compromised.[5].

13.7.3 This 72-hour time period shall not commence during the initial assessment (investigation) to determine whether or not a breach occurred.

13.7.4 Where the Organisation has been notified of a breach by third party Operators, the Organisation is deemed to have reasonable certainty**.**

Information Regulator and Affected Individuals

13.7.5 POPI requires that where there are reasonable grounds to believe that a breach has occurred, the Organisation must notify the Information Regulator and affected Individuals. Given this overbroad and overburdening obligation, the Organisation shall adopt the risk-based approach to notification of the Information Regulator using the results of the risk assessment in Step 3.

[5] Section 22 of POPI requires notification to be made as soon as reasonably possible after the discovery of the compromise.

Scope of notification: All data breaches likely to result in risk to rights and freedoms of Data Subject.

a) No likely risk → No notification
b) Likelihood of risk Notify the Information Regulator
c) Likelihood of high risk Notify both the Information Regulator and affected individuals.

13.7.6 The **Step 3: Risk assessment** must be documented by the Information Officer regardless of risk level or notification obligations and shall further include reasons for not notifying the Information Regulator and/or affected individuals. The Information Officer must retain the records in relation thereto in a central records repository.

13.7.7 Notification to affected individuals shall not be required if appropriate measures render the data unintelligible or render the high risk unlikely to materialise.

Methods of Notification

13.7.8 Notifying the Information Regulator

a) All contact with the Information Regulator shall occur through the Information Officer, by way of email and must not involve the communication of personal data.
b) Where notification has not occurred within 72 hours, the notification shall include the reasons for not doing so.
c) Where notification to the Information Regulator is appropriate, the Information Officer shall submit the Incident Report together with a recommendation with regard to the measures to be taken by individuals to mitigate the possible adverse effects of the compromise.

13.7.9 Notifying affected individuals

a) The Information Officer must firstly consider who to notify.

b) The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves. This is the underlying principle for why individuals are being notified.

c) As a minimum POPI requires the following information to be included in this notification:

(i) a description of the possible consequences of the security compromise;

(ii) a description of the measures that the Responsible Party intends to take or has taken to address the security compromise;

(iii) a recommendation with regard to the measures to be taken by the individual to mitigate the possible adverse effects of the security compromise;

(iv) if known to the Organisation, the identity of the unauthorised person who may have accessed or acquired the personal information; and

(v) Contact information for further details.

d) In deciding how to communicate the notification to individuals, the Information Officer must consider, in consultation with the head of the Organisation's media/public relations department what is appropriate in the circumstances. In this regard:

(i) a large number of affected individuals is indicative that a public press release may be more appropriate opposed to individual communication.

(ii) if sensitive personal information is compromised individual communication is preferable.

(iii) It must be determined whether legal advice is required in preparing such notification.

13.8 Step 6: Evaluation and response

13.8.1 Subsequent to a personal data security breach, the Information Officer must, in consultation with the Organisation's stakeholders, reflect on the

incident with the purpose of ensuring that the steps taken were appropriate and where improvements are required.

13.8.2 In the case of a serious breach (i.e. risk level 2b and above), the aforesaid parties must review:

a) What action needs to be taken to reduce the risk of future breaches and to minimise the potential impact thereof?
b) Whether policies, procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
c) Are there weak points in security controls that need to be strengthened?
d) Are staff and users of services aware of their responsibilities for information security and adequately trained?
e) Is additional investment required to reduce exposure?

13.8.3 The Board, together with the Information Officer, is to consider whether it is appropriate to pursue any civil or criminal legal proceedings against individuals or groups and/or any disciplinary proceedings against Employees of the Organisation.

14 RECORDS

14.2 The Information Officer shall compile and maintain a central records repository of all personal data breaches and will report on incidents to the Board at least on a quarterly basis in order to identify lessons learned, patterns of incidents and evidence of weakness that need to be addressed. All level 2b and 3 breaches shall be recorded by the Disaster Project Team in the disaster recovery register.

14.3 All consultations and communications should be recorded or reduced to writing as soon as reasonably practicable.

14.4 The central records repository shall include all assessments, forms and minutes conducted in accordance with Step 1 to Step 6.

14.5 Tasks of the Information Officer include the following:

14.5.1 to inform and advise the Information Officer or the processor and the employees who carry out processing of their obligations pursuant to the POPIA and any other applicable laws relating to data protection provisions;

14.5.2 to monitor compliance with applicable laws and Regulations data protection provisions and with the policies of the Information Officer or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

14.5.3 to provide advice where requested as regards the data protection impact assessment and monitor its performance;

14.5.4 to cooperate with the supervisory authority;

14.5.5 to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation; and

14.5.6 to consult, where appropriate, with regard to any other matter.

14.5.7 the Information Officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

15 APPENDIX A

DATA SUBJECT CONSENT

General

The Organisation Earth Touch (Pty) Ltd Registration Number: 2006/014191/07 Contact details:	**Information Officer : Lara Cox** E-mail Address: lcox@earthtouchsa.com Telephone Number during office hours (08H00 – 17H00) (Tel: +44 74 717198209)

	Reason for requesting Personal Information	**Applicable Yes / No**	**Further explanation of request for Personal Information**	**Consent Yes / No**
1.	Personal Information of applicants for employment or internship with the Organisation for the purposes of confirming, verifying personal details, contacting, consideration, appointment and performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship where applicable as well as for legislative audit and record keeping purposes and compliance with legal and regulatory requirements (eg. Tax and labour law)		[redacted]	
2.	Personal Information of its contractors for the purposes of confirming, verifying and updating the Person's details, contracting in respect of transactions, audit and record keeping purposes.			
3.	Personal Information of its suppliers for the purposes of confirming, verifying and updating the Peron's details, contracting in respect of transactions, audit and record			

	keeping purposes			
4.	Personal Information that is necessary for compliance with a legal obligation to which the Organisation is subject		*(Describe the legal obligation)*	
5.				
6.				
7.	Personal Information that is necessary for the purposes of the legitimate interests pursued by the Organisation or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Information, in particular where the Data Subject is a child[6].		*(Describe the legitimate interests being pursed)*	
8.	Any other: *(Describe)*			
9.	Describe any consequences for the Data Subject in providing the Personal Information:			
10.	Employees of the Organisation who process the Personal Information will receive the Personal Information subject to confidentiality statements or agreements with the Organisation			
11.				
12.	Personal Information will be stored for a period of 5 years			
13.	Consent may be withdrawn at any time, but this won't affect the lawfulness of processing based on consent before its withdrawal			

[6] General Data Protection Regulations: Article 6 (Lawfulness of processing)

14.	Complaints may be lodged with: The Information Regulator of South Africa or such body as determined by the GDPR whichever may be applicable			
15.	Consequences of failure to provide the required Personal Information:			
16.	Personal Information may be erased on request of the Data Subject, subject to the provisions of the Protection of Personal Information Act 4 of 2013 as amended from time to time, read with the GDPR (article 17) as may be applicable to the Data Subject.			
17.	The Organisation shall act on any request by a Data Subject in relation to the Data Subject's Personal Information, unless the Organisation cannot identify the Data Subject. The Organisation shall provide information on action taken on a request by the Data Subject without undue delay and within 1 month of receipt of the request. The period may be extended by another 2 months where necessary, taking into account the complexity and number of the requests. The Organisation shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where requests are manifestly unfounded or excessive, the Organisation may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request.			
	GDPR means the General Data Protection Regulation			

Name of Data Subject	
Signature of Data Subject	
Date	

Website consent

(to be included in website terms and conditions of use, which must be updated from time to time)

"At all times, Your personal information will be handled and/or processed in accordance with statutory provisions governing personal information.

Earth Touch is sensitive to the private nature of the information a User provides over the Website, including a User's name, company details, address and email address, and shall take all reasonable steps to protect the personal information of the User.

Any personal information provided by You to Earth Touch may be used by Earth Touch:

to operate, maintain, and improve the features and functionality of the Website and/or Your account;

to develop new products and services;

to provide marketing with aggregate information about the user base and usage patterns;

for internal administrative purposes;

for statistical purposes; and

to send You information regarding Earth Touch;

will not:

be used by Earth Touch to send commercial or marketing messages to You without Your prior consent, other than in the circumstances described in clauses 5.3[7] and 8.3.1.6[8];

be sold, shared, made available or transmitted to any third parties;

[7] 5.3 Certain third party vendors and/or advertising networks whose advertisements may appear on the Website, and other websites, may make use of cookies, and may serve and select advertisements based on Your browsing history, including Your prior visit(s) to the Website and/or other websites on the internet.5.3.1. The cookies gathered by such third party vendors and/or advertisement networks may be used to display advertisements to You on the Website based on the information contained in the cookies that such third party vendors and/or advertisement networks have gathered 5.3.2. If You do not agree with the use of cookies, or the gathering of your private browsing data through the use of cookies, you should: 5.3.2.1. visit the third party vendor's website to familiarize yourself with their cookie policy and to opt-out of their use of cookies where this is possible; 5.3.2.2. amend your browser settings to disable cookies (Please note that this may affect your user experience on certain websites); or 5.3.2.3. refrain from using websites that use cookies in a manner that you do not agree with; and, 5.3.2.4. visit aboutads.info should you require any further information on the subject.

[8] To send You information regarding Earth Touch.

through Your account is stored by Earth Touch on a secure database.

Despite the foregoing, You agree that Earth Touch is entitled to disclose any personal information to any competent legal or regulatory authority that makes such a request and is lawfully entitled to obtain such information from Earth Touch. In this instance, Earth Touch undertakes to disclose only such information as is sufficient to satisfy such request.

Employees of Earth Touch who process your personal information will receive the Personal Information subject to confidentiality agreements with Earth Touch.

Your personal information will be stored for a period of 5 years

Your consent may be withdrawn at any time, but this does not affect the lawfulness of processing based on consent before its withdrawal.

Complaints may be lodged with:
Information Officer
E-mail Address: lcox@earthtouchsa.com
Telephone Number during office hours (08H00 – 17H00) +27 31 5820800
Telephone Number outside of office hours (Tel/Mobile: +44 74717198209
OR
Regulator

If You choose not to provide us with your consent to process the personal information required, we shall not be able to allow you further access to our website nor be able to receive information from Earth Touch.

Your personal information may be erased at Your request, subject to the provisions of the Protection of Personal Information Act, read with the GDPR (article 17) as may be applicable to the Data Subject.

Earth Touch shall act on any request by yourself in relation to Your personal information, unless the Earth Touch cannot identify You. Earth Touch shall provide information on action taken on a request by yourself without undue delay and within 1 month of receipt of the request. The period may be extended by another 2 months where necessary, taking into account the complexity and number of the requests. Earth Touch shall inform you of any such extension within one month of receipt of the request, together with the reasons for the delay. Where any such requests are manifestly unfounded or excessive, the Earth Touch may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request.

16 APPENDIX B

APPENDIX A – PERSONAL / OTHER CONFIDENTIAL DATA SECURITY BREACH REPORT FORM

Heads of Department (either Finance or Production) to complete PART 1 of this form and email it to the Information Officer at: lcox@earthtouchsa.com

Part 1:	**Notification of Data Security Breach: To be completed by person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number)	
Brief description of incident or details of the information lost	
Details of the IT systems, equipment, devices, records involved in the security breach:	

Number of Data Subjects (individuals) affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	

For Completion by Information Officer
Received by:
On (date):
Forwarded for action to:
On (date):

PART 2: Assessment of Severity	**To be completed by Information Officer in consultation with Head of Department (either Finance or Production) affected by the breach**
Details of information loss:	
If laptop lost/stolen: how recently was the laptop backed up onto IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Organisation or third parties?	
Is the data bound by any contractual confidentiality or non-disclosure arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	

HIGH RISK personal data **A. Special Categories of personal data** relating to a living, identifiable individual's: a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) membership of a trade union; e) genetic or biometric data; f) data concerning health; g) data concerning a person's sex life or sexual orientation; h) criminal convictions/offences.	
B. Information that could be used to commit identity fraud such as: a) personal bank account information; b) other financial information; c) copies of identity documents or numbers; d) copies of visas or passports.	
C. Personal information relating to vulnerable adults and children;	
D. Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
E. Performance evaluation information, disciplinary information which could adversely affect individuals.	
F. Commercially sensitive information or negotiations which could adversely	

affect individuals	
G. Security information that would compromise the safety of individuals if disclosed.	
Initial Risk Category of incident (1, 2a, 2b or 3):	
Signature of Information Officer	Signature of Head of Department

PART 3: ACTION TAKEN	**To be completed by Information Officer**
If notified to Information Regulator, provide details, including date:	
If notified to Data Subjects, provide details, including date:	
If notified to other external party, regulator/stakeholder, provide details:	
If reported to SAPS, provide details, including dates and case number (if any).	

If notified to other internal stakeholders, provide details and dates:	
Follow up action required/recommended:	

CHECKLIST FOR ASSESSING SEVERITY OF THE INCIDENT

<u>Level 1: Local Incident</u>:

- Is this a local incident?

  **Local incident is limited disruption to services (department or Organisation) or no serious threat to life, property or the environment and no threat to the Organisation's reputation.*

- Can the consequences of the security breach, loss or unavailability of the asset be managed locally within normal operating procedures?

- If so, manage the incident according to the Data Security Breach Management Protocol

Level 2.a: Minor Disaster – Unlikely to Escalate into a Major Disaster:

- Is this a Minor Disaster?
    - "**Minor Disaster**" is a disruption to the functioning capacity of a key Organisation building or a key service. The incident poses a threat to life, property or environment, at a minor level but may escalate to a Major Disaster.

- Does containment and recovery require assistance from other members of staff within the Organisation or external specialist support teams?

- Does the breach require a notification to the Organisation's senior managers?

- If so, the Information Officer will decide who else needs to assist or be made aware of the breach. For example:

    - Chief Executive Officer of the Organisation
    - Information Technology Manager

Risk Level 2.b: Minor Disaster or Level 3: Major Disaster

- Is this a major incident?
- Does containment and recovery, or the consequences of the loss or unavailability of the asset, require significant Organisational resources beyond normal operating procedures?
- If so, inform the Disaster Project Team who will follow the Organisation's Disaster Recovery Policy and Plan in terms of the Information Management Policy.

Guide to defining incident levels:

- Does the incident need to be reported immediately to the SAPS?
- How important an information asset is to the Organisation's business process or function
- Whether the asset is a vital record. Is it unique – once lost, lost forever?
- Will its loss have adverse financial legal, liability or reputational consequences?

- Is it business-critical? Do you rely on access to this particular information asset or you can turn to reliable electronic copies or alternative manual processes.
- Does the loss or breach of data security involve high risk personal data (i.e. Sensitive Personal Information).