AFRICAN EQUITY EMPOWERMENT INVESTMENTS LIMITED
("AEEI")

PROTECTION OF PERSONAL INFORMATION POLICY

Date of Issue: 28 JULY 2021

TABLE OF CONTENTS

PART 1: GENERAL PRINCIPLES

1 POLICY STATEMENT

1.1 The purpose of this Policy is to develop and secure sound and sustainable management of the processing of Personal Information and, where relevant, Special Personal Information within AEEI by establishing principles, norms, standards and other requirements to –

1.1.1 regulate the processing of Personal Information and, where relevant, Special Personal Information in a manner which complies with the provisions of the Act and gives effect to the right to privacy as envisaged in section 14 of the Constitution of the Republic of South Africa Act, No 108 of 1996, subject to justifiable limitations;

1.1.2 govern the manner in which Personal Information is collected, stored, recorded and transferred regardless of the form or medium thereof;

1.1.3 regulate and prescribe the retention of Records and the periods thereof; and

1.1.4 ensure compliance with all other relevant legislation which governs the processing of Personal Information.

1.2 Employees and other parties who are bound by or otherwise required to recognise and abide by this Policy who compromise or violate the provisions of this Policy could significantly damage AEEI's interests, including its relationships with third parties and its reputation, and expose it to un-intended legal and commercial consequences, risks and liabilities. Accordingly, any violation of this Policy will be subject to appropriate action by the relevant AEEI company, including *inter alia* possible termination of employment or damages claims, should circumstances so require.

2 DEFINITIONS

2.1 In this Policy, unless otherwise indicated by the context, the following terms shall have the meaning ascribed to them –

2.1.1 "**Act**" means the Protection of Personal Information Act, No 4 of 2013, as amended from time to time;

2.1.2 "**AEEI**" or "**Company**" means African Equity Empowerment Investments Limited, registration number 1996/006093/06, a public company duly registered in the Republic of South Africa;

2.1.3 "**Board**" means the board of directors of AEEI, from time to time, or if there is only one director, then that director;

2.1.4 "**CIPC**" means the Companies and Intellectual Property Commission established in terms of section 185 of the Companies Act;

2.1.5 "**Companies Act**" means the Companies Act, No 71 of 2008, as amended from time to time;

2.1.6 "**Consent**" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;

2.1.7 "**Data Subject**" means the person to whom the Personal Information relates;

2.1.8 "**Deputy Information Officers**" means those persons contemplated in paragraph 7.2;

2.1.9 "**Employees**" means individuals employed by any company within AEEI;

2.1.10 "**Information Officer**" means the individual contemplated in paragraph 7.2.1;

2.1.11 "**Operator**" means a person who processes Personal Information for AEEI in terms of a contract or mandate, without coming under the direct authority of AEEI;

2.1.12 "**PAIA**" means the Promotion of Access to Information Act, No 2 of 2000, as amended from time to time;

2.1.13 "**Personal Information**" means personal information as defined in the Act as contemplated in paragraph 10.1;

2.1.14 "**Policy**" means the policy set out in this document and includes all annexures hereto (if any) and any sub-policies prepared from time to time, as amended or revised from time to time;

2.1.15 "**processing**" means processing as contemplated in paragraph 4.3;

2.1.16 "**public body**" means public body as defined in the Act;

2.1.17 "**Record**" means a record as defined in the Act and currently comprising of any recorded information –

2.1.17.1 regardless of form or medium, including any of the following –

2.1.17.1.1 writing on any material;

2.1.17.1.2 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;

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

2.1.17.1.4 book, map, plan, graph or drawing;

2.1.17.1.5 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 of some other equipment, of being reproduced;

2.1.17.2 in the possession or under the control of a responsible party;

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

2.1.17.4 regardless of when it came into existence;

2.1.18 "**Regulations**" means the Regulations relating to the Protection of Personal Information published in accordance with the provisions of the Act in Government Gazette No. 42110;

2.1.19 "**Regulator**" means the information regulator established in terms of section 39 of the Act;

2.1.20 "**Responsible Party**" bears the definition accorded to it in section 1 of the Act;

2.1.21 "**South Africa**" means the Republic of South Africa;

2.1.22 "**Special Personal Information**" means Personal Information concerning –

2.1.22.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or

2.1.22.2 the criminal behaviour of a Data Subject to the extent that such information relates to -

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

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

2.1.22.2.3 any Personal Information concerning a child being 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.

2.2 In this Policy —

2.2.1 paragraph headings and the heading of the Policy are for convenience only and are not to be used in its interpretation;

2.2.2 an expression which denotes —

2.2.2.1 any gender includes the other genders;

2.2.2.2 a natural person includes a juristic person and *vice versa*;

2.2.2.3 the singular includes the plural and *vice versa*;

2.2.2.4 a Party includes a reference to that Party's successors in title and assigns allowed at law; and

2.2.2.5 a reference to a consecutive series of two or more paragraphs is deemed to be inclusive of both the first and last mentioned paragraphs.

2.3 Any reference in this Policy to –

2.3.1 "**days**" shall be construed as calendar days unless qualified by the word "business", in which instance a "business day" will be any day other than a Saturday, Sunday or public holiday as gazetted by the government of the Republic of South Africa from time to time;

2.3.2 "**laws**" means all constitutions; statutes; regulations; by-laws; codes; ordinances; decrees; rules; judicial, arbitral, administrative, ministerial,

departmental or regulatory judgements, orders, decisions, rulings, or awards; policies; voluntary restraints; guidelines; directives; compliance notices; abatement notices; agreements with, requirements of, or instructions by any Governmental Body; and the common law, and "**law**" shall have a similar meaning; and

2.3.3 "**person**" means any person, company, close corporation, trust, partnership or other entity whether or not having separate legal personality.

2.4 The words "**include**" and "**including**" mean "include without limitation" and "including without limitation". The use of the words "**include**" and "**including**" followed by a specific example or examples shall not be construed as limiting the meaning of the general wording preceding it.

2.5 Words and expressions defined in any paragraph shall, unless the application of any such word or expression is specifically limited to that paragraph, bear the meaning assigned to such word or expression throughout this Policy.

2.6 Unless otherwise provided, defined terms appearing in this Policy in title case shall be given their meaning as defined, while the same terms appearing in lower case shall be interpreted in accordance with their plain English meaning.

2.7 A reference to any statutory enactment shall be construed as a reference to that enactment as at the date of issue or date of revision as the case may be and as amended or substituted from time to time.

2.8 Unless specifically otherwise provided, any number of days prescribed shall be determined by excluding the first and including the last day, and where the last day falls on a day that is not a business day, the next succeeding business day.

2.9 No provision of this Policy shall (unless otherwise stipulated) constitute a stipulation for the benefit of any person (*stipulatio alteri*) who is not a Party to this Policy.

2.10 Any reference in this Policy to "**this Policy**" or to any other policy or document shall be construed as a reference to this Policy or, as the case may be, such other policy or document, as amended, varied, novated or supplemented from time to time.

2.11 In this Policy the words "**paragraph**" or "**paragraphs**" and "**annexure**" or "**annexures**" refer to paragraphs of and annexures to this Policy.

3 INTRODUCTION

3.1 AEEI is a majority black-owned and black-controlled investment holding company with a diversified investment portfolio. AEEI's investments include fishing and brands, technology, biotherapeutics, health and beauty, events and tourism as well strategic investments.

3.2 During the course and scope of its business activities AEEI obtains Personal Information from a variety of sources including customers, Employees, suppliers and various third parties who may engage with AEEI from time to time.

3.3 The Act governs the processing of Personal Information, including but not limited to Special Personal Information and imposes certain obligations on AEEI in relation to this information and the manner in which it is processed.

3.4 Accordingly, AEEI wishes to govern, regulate and administer the processing of Personal Information through this Policy in order to comply with the provisions of the Act.

3.5 AEEI Employees and other officials, agents, representatives of AEEI shall be bound by and be required to observe and implement this Policy at all times.

4 BACKGROUND TO THE ACT

4.1 The Act aims to give effect to the constitutional right to privacy by safeguarding Personal Information when processed by a Responsible Party. The Act sets forth various provisions which will, *inter alia*, regulate the manner in which Personal Information may be processed.

4.2 The Act will apply to the processing of Personal Information entered in a Record by or on behalf of a Responsible Party, where such Responsible Party is either domiciled in the Republic or, is domiciled outside of South Africa, but makes use of the automated or non-automated means in South Africa, unless those means are used only to forward Personal Information within South Africa.

4.3 For the purposes of the Act, "processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including –

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

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

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

4.4 The Act prescribes certain conditions for the lawful processing of Personal Information which can be summarised as follows –

4.4.1 Condition 1: Accountability: the Responsible Party (i.e. in this instance, AEEI) must ensure that measures are taken which give effect to the conditions set out in the Act.

4.4.2 Condition 2: Processing Limitation: Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of a Data Subject. Personal Information may only be processed if, given the purpose for which it is processed, the processing is adequate, relevant and not excessive. Further, subject to certain exceptions, Personal Information may only be processed with the Consent of a Data Subject and must be collected directly from a Data Subject.

4.4.3 Condition 3: Purpose Specification*:* Personal Information must be collected for a specific, explicitly defined and legitimate purpose. Personal Information may also not be kept for longer than is necessary for achieving the purpose for which it is collected or subsequently processed.

4.4.4 Condition 4: Further Process Limitation: Personal Information must not be further processed in a way incompatible with the purpose for which it was originally collected.

4.4.5 Condition 5: Information Quality: The Responsible Party must take reasonable practical steps to ensure that the Personal Information is complete, accurate, not misleading, and updated where necessary.

4.4.6 Condition 6: Openness: The Responsible Party must maintain the documentation for all processing operations in accordance with its responsibility referred to in sections 14 and 51 of PAIA. Further, if Personal Information is collected, the Responsible Party must take reasonably practicable steps to ensure that the Data Subjects are, *inter alia*, aware of the information being collected and the purpose for such collection.

4.4.7 Condition 7: Security Safeguards: Appropriate technical and organisational measures must be taken to secure the integrity of Personal Information by safeguarding against the risk of loss or

damage or destruction of Personal Information and against the unauthorised or unlawful access to, or processing of Personal Information.

4.5 We will refer to these conditions where relevant herein and particularly the applicability thereof to the activities of AEEI.

5 PURPOSE

5.1 AEEI is exposed to Personal Information (including, without limitation, Special Personal Information) in its day-to-day activities. Our clients and Employees in particular, need to be able to trust us with the information they provide to us. AEEI must, accordingly, respect and protect the integrity of the Personal Information it holds by, in particular, treating it with care and keeping it confidential.

5.2 The goal of this Policy is to ensure that Personal Information is processed and recorded in accordance with the provisions of the Act, whilst still enabling AEEI to use the Personal Information for lawful and legitimate purposes in the furtherance of its business aims and objectives.

6 APPLICATION, COMMENCEMENT AND OBJECTIVES

6.1 Application

6.1.1 This Policy applies to the processing of all Personal Information (including, without limitation, Special Personal Information) by or on behalf of AEEI, by all Employees, officials, agents, and representatives of AEEI. The processing of Personal Information (including, without limitation, Special Personal Information) must comply with the provisions of this Policy read in conjunction with the Act and the Regulations.

6.1.2 This Policy prevails over all other policies of AEEI pertaining to the processing of Personal Information (including, without limitation, Special Personal Information). All persons involved in the processing and recording of Personal Information shall –

6.1.2.1 comply with the relevant provisions of the Act and the Regulations as read with this Policy;

6.1.2.2 interpret and apply this Policy congruently with any other policies of AEEI to the extent that such congruency is possible;

6.1.2.3 apply this Policy in preference to any other policies of AEEI in the event that ambiguity and/or conflict and/or vagueness exists between this Policy and other policies of AEEI.

6.1.3 AEEI must, however, use its best endeavours to ensure that all other policies confirm and are aligned with the terms and conditions set out herein where relevant.

6.2 **Commencement**

This Policy shall come into effect on **[insert date]**.

6.3 **Objectives**

6.3.1 The objectives of this Policy are to ensure that the processing of Personal Information (including, without limitation, Special Personal Information) by AEEI –

6.3.1.1 complies with all applicable legislation, including (without limitation) the Act and the Regulations; and

6.3.1.2 occurs in a manner that facilitates and enhances the ability of AEEI to achieve its objectives but with due regard to safeguarding the interests of Data Subjects in relation to their Personal Information.

6.3.2 This Policy also strives to ensure that consistency is achieved and maintained in relation to the processing of Personal Information (including, without limitation, Special Personal Information) throughout AEEI at all times.

7 OVERSIGHT AND RESPONSIBILITIES

7.1 **General**

7.1.1 The Board is generally responsible for the management oversight and control of the activities of AEEI.

7.1.2 The executive management team is, however, responsible for day to day management.

7.1.3 The Board shall ensure that the terms and conditions set out in this Policy are observed at all times by introducing and maintaining the appropriate procedures and deploying the appropriate resources to achieve this.

7.2 **Information Officer and Deputy Information Officers**

7.2.1 The Information Officer for AEEI is the **[insert position]**, **[insert name]**.

7.2.2 The Information Officer may designate certain individuals as Deputy Information Officers within the Company and, accordingly, certain of the duties and responsibilities of the Information Officer may be delegated to such Deputy Information Officers.

7.2.3 The Information Officer will be deemed to have delegated, on a revocable basis, aspects of his authority to the Deputy Information Officers in respect of the following matters –

7.2.3.1 to provide general guidance on the processing and recording of Personal Information (including, without limitation, Special Personal Information) in accordance with this Policy as read with the Act;

7.2.3.2 to encourage the compliance by AEEI, each department or business unit therein, as well as all Employees, with the conditions for the lawful processing of Personal Information (including, without limitation, Special Personal Information);

7.2.3.3 dealing with requests made to AEEI pursuant to the Act as well as this Policy;

7.2.3.4 working with the Regulator in respect of any investigations conducted pursuant to the Act in relation to AEEI;

7.2.3.5 to otherwise ensure compliance by AEEI, each department or business unit therein, as well as all Employees, with the provisions of the Act, the Regulations and this Policy; and

7.2.3.6 to generally implement all processing activities in accordance with this Policy as read with the Act and the Regulations.

7.2.4 The Information Officer and Deputy Information Officers shall only be required to perform the functions contemplated in paragraph 7.2.3 upon the Information Officer being registered with the Regulator.

8 REPORTING

8.1 Information Officer's Report

8.1.1 The Information Officer shall submit a report on the implementation of this Policy to the Board upon the request of the Board. Such report shall deal, *inter alia*, with –

8.1.1.1 the compliance of all divisions and business units with the provisions of this Policy;

8.1.1.2 the implementation of relevant security safeguards for the protection of the Personal Information as contemplated in paragraph 16;

8.1.1.3 any security compromises in which there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by an unauthorised third party;

8.1.1.4 any complaints received in respect of the processing of Personal Information as well as any unauthorised use of the Personal Information (including, without limitation, Special Personal Information) of a Data Subject by anyone in AEEI; and

8.1.1.5 any and all other matters as may be appropriate and/or necessary to be addressed in the report contemplated in this paragraph 8.1.

8.1.2 The Deputy Information Officers, in accordance with the provisions of paragraph 16.4, shall immediately report any compromises in AEEI's security safeguards in writing to the Information Officer, and whereupon the Information Officer shall be obliged to immediately report same to the Board.

9 ETHICAL OBLIGATIONS AND STANDARDS

9.1 Employees shall be obliged to observe the following duties so as to act in the best interests of AEEI and in due cognisance of the right to privacy of Data Subjects at all times during the processing of Personal Information and after the completion thereof –

9.1.1 Employees shall not exceed the powers conferred upon them in terms of the Act, the Regulations, this Policy and their respective employment agreements;

9.1.2 Employees shall not exercise their powers for an improper or collateral purpose by abusing their positions as employees or office bearers of AEEI in order to derive personal or private benefit or advantage; and

9.1.3 Employees shall avoid a conflict between the interests of AEEI and their personal or private interests or benefit.

9.2 In the event that an Employee breaches any terms or conditions of this Policy, AEEI shall be entitled, without prejudice to any of its rights in terms of this Policy or at law, to take such action against such Employee in terms of any disciplinary code which AEEI may have in place or the relevant code of conduct or behaviour that applies to such Employee.

PART 2: PROCESSING AND RECORDING

10 GENERAL

10.1 Personal Information is defined by the Act as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing, juristic person, including, but not limited to –

10.1.1 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;

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

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

10.1.4 the biometric information of the person;

10.1.5 the personal opinions, views or preferences of the person;

10.1.6 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;

10.1.7 the views or opinions of another individual about the person; and

10.1.8 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.

10.2 Subject to the provisions of the Act, Personal Information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address and telephone number and does not include information made lawfully available to the general public.

10.3 **Collection of Personal Information**

10.3.1 Subject to the provisions of paragraph 10.4 as read with the Act, Personal Information must be collected directly from the Data Subject. This includes all Personal Information required from clients and

prospective clients as well as all customers, Employees and third parties applying for positions within AEEI or rendering services to AEEI.

10.3.2 Any request (which will include, but not be limited to all application forms as well as other information requests, in whatsoever medium or format) to a Data Subject for Personal Information must be in writing and contain at least the following –

10.3.2.1 details pertaining to the Personal Information being collected and, where the Personal Information is not collected from the Data Subject, the source from which it is collected;

10.3.2.2 the name and address of AEEI;

10.3.2.3 the purpose for which the Personal Information is being collected;

10.3.2.4 whether or not the supply of the Personal Information by that Data Subject is voluntary or mandatory;

10.3.2.5 the consequences of failure to provide the Personal Information;

10.3.2.6 any particular law authorising or requiring the collection of the Personal Information;

10.3.2.7 whether the Personal Information will or may be transferred to a third party residing outside of South Africa and the level of protection afforded to the Personal Information by that non-resident third party;

10.3.2.8 the recipient or category of recipients of the Personal Information;

10.3.2.9 the nature or category of the Personal Information;

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

10.3.2.11 the existence of the right to object to the processing of Personal Information; and

10.3.2.12 the existence of the right to lodge a complaint to the Regulator and the contact details of the Regulator.

10.4 Notwithstanding the provisions of paragraph 10.3.2 above, there may be instances where a request for Personal Information will be made telephonically by the Company to the Data Subject. In these instances, the Company shall ensure that the Data Subject is verbally informed of the information listed in paragraph 10.3.2 above.

10.5 Notwithstanding the provisions of paragraph 10.3.1, Personal Information need not be collected directly from the Data Subject in the event that –

10.5.1 the Personal Information is derived from a public record or has been deliberately made public by the Data Subject. A public record is defined in the Act as 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. Examples of public records include deeds office records and CIPC records;

10.5.2 the Data Subject or, where the Data Subject is under the age of 18 (eighteen), his or her parent and/or guardian has consented to the collection of the Personal Information from another source;

10.5.3 the collection of Personal Information from another source would not prejudice a legitimate interest of the Data Subject;

10.5.4 the collection of the Personal Information from another source is necessary –

10.5.4.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

10.5.4.2 to comply with an obligation imposed by law or enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, No 34 of 1997;

10.5.4.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

10.5.4.4 in the interest of national security; or

10.5.4.5 to maintain the legitimate interests of AEEI or of a third party to whom the information is supplied;

10.5.5 the collection would prejudice the lawful purpose thereof; or

10.5.6 it is not reasonably practical in the circumstances of the particular case.

10.6 **Requests for Personal Information**

Any person who receives a written request from a Data Subject to obtain a Record or description of the Personal Information held by AEEI about the Data Subject, shall be required to –

10.6.1 obtain a certified copy of the proof of identification of that Data Subject; and

10.6.2 refer such request to the Information Officer who must deal with such request in the manner and form prescribed in terms of the Act, as well as PAIA**.**

10.7 **Correction of Personal Information**

10.7.1 A Data Subject is entitled to provide AEEI with a written request to –

10.7.1.1 correct or delete the Personal Information about the Data Subject in the possession or control of AEEI which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

10.7.1.2 destroy or delete a Record of Personal Information about the Data Subject that AEEI is no longer authorised to retain.

10.7.2 Within 20 business days (or if this period is not reasonable, then such extended period as may be reasonable in the circumstances) of receipt of the written request contemplated in paragraph 10.7.1, the relevant person so designated by the Information Officer shall –

10.7.2.1 correct the Personal Information;

10.7.2.2 destroy or delete the Personal Information;

10.7.2.3 provide the Data Subject, subject to his or her satisfaction, with credible evidence in support of the Personal Information; or

10.7.2.4 where agreement cannot be reached between AEEI and the Data Subject concerned, and if the Data Subject so requests, take such steps, as are reasonable in the circumstances, to attach to the Personal Information in such a manner that it will always be read with the Personal

Information, an indication that a correction of the Personal Information has been requested but not been made.

10.7.3 In the event of the Information Officer having taken steps as contemplated in paragraphs 10.7.1 and 10.7.2, where such steps have resulted in a change to the Personal Information of the Data Subject, and where the changed Personal Information has an impact on decisions that have been or will be taken in respect of the Data Subject in question, the Information Officer must, if reasonably practicable, and within 20 business days (or if such period is not reasonable then such extended period as may be reasonable in the circumstances) of such amendment taking place, inform each person or body to whom the Personal Information has been disclosed of the steps taken.

11 PROCESSING OF PERSONAL INFORMATION

AEEI has a general and overriding duty to ensure that, at the time of determining the purpose and means of processing of any Personal Information of a Data Subject, as well as during the processing of the aforesaid, the provisions contemplated in this paragraph 11 as read with the Act, are complied with.

11.1 Consent, Justification and Objection

11.1.1 For Personal Information to be lawfully processed by AEEI, one of the following requirements must be complied with, namely that –

11.1.1.1 the Consent of the Data Subject to such processing must be obtained, or in the case of the Data Subject being under the age of 18, the parent and/or guardian of such Data Subject must provide his or her Consent to the processing;

11.1.1.2 the processing of the Personal Information is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party;

11.1.1.3 the processing complies with an obligation imposed by law on AEEI;

11.1.1.4 the processing protects a legitimate interest of the Data Subject.

11.1.1.5 the processing is necessary for the proper performance of a public law duty by a public body; or

11.1.1.6 the processing is necessary for pursuing the legitimate interests of AEEI or a third party to whom the Personal Information is supplied.

11.1.2 The Consent contemplated in paragraph 11.1.1.1 may be withdrawn by the Data Subject or, where relevant, the parent and/or guardian of the Data Subject, at any time. Such withdrawal shall be made in writing to the Information Officer. The Data Subject is to be informed of this requirement. Where the Data Subject has withdrawn his or her Consent, the Personal Information of such Data Subject should no longer be processed.

11.1.3 The withdrawal of Consent as contemplated above shall not affect the lawfulness of the processing of the Personal Information either in terms of paragraphs 11.1.1.2 to 11.1.1.6 or which took place prior to AEEI receiving notification of such withdrawal.

11.1.4 Except where such processing is required in terms of legislation, the Data Subject may, at any time, object to the processing of Personal Information in terms of paragraphs 11.1.1.2 to 11.1.1.6, on reasonable grounds relating to his or her particular situation. Such notice of objection is to be made in writing to the Information Officer. Where AEEI receives notice of such objection as contemplated herein, AEEI may no longer process the Personal Information of the objecting Data Subject.

11.2 **Further processing**

11.2.1 Further processing of Personal Information must be in accordance with the purpose for which the information was collected. Where this is not the case, the Consent of the Data Subject to such further processing must be obtained.

11.2.2 In assessing whether further processing is compatible with the purpose of collection, AEEI shall take account of –

11.2.2.1 the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

11.2.2.2 the nature of the information concerned;

11.2.2.3 the consequences of the intended further processing for the Data Subject;

11.2.2.4 the manner in which the Personal Information has been collected; and

11.2.2.5 any contractual rights and obligations between the parties.

11.2.3 Notwithstanding the provisions of paragraph 11.2.1, in the event of –

11.2.3.1 the information being available in or derived from a public record or having deliberately been made public by the Data Subject;

11.2.3.2 the further processing being necessary: (i) to avoid prejudice to the maintenance of the law by any public body; (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue; (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or (iv) in the interests of national security;

11.2.3.3 the further processing being necessary to prevent or mitigate a serious and imminent threat to public health, public safety or the life or health of the Data Subject; or

11.2.3.4 the Personal Information being used for historical, statistical or research purposes and AEEI ensures that the further processing is carried out solely for such purpose and will not be published in an identifiable form,

the further processing of such Personal Information may take place without the Consent of the Data Subject or his or her parent and/or guardian, where applicable.

11.3 **Restrictions**

11.3.1 AEEI shall be required to place restrictions on the processing of Personal Information in the event of –

11.3.1.1 the accuracy of the Personal Information being contested by the Data Subject, for a period to verify the accuracy of the information;

11.3.1.2 AEEI no longer requiring the Personal Information for achieving the purpose for which it was collected or subsequently processed, but such information is being retained for purposes of proof;

11.3.1.3 the processing being unlawful and the Data Subject, opposing the destruction or deletion thereof, requesting for the restriction of the use of the Personal Information; or

11.3.1.4 the Data Subject requests to transmit the personal data into another automated processing system.

11.3.2 Where a restriction as contemplated in this paragraph 11.3 has been placed on the processing of the Personal Information of a Data Subject, such information may, with the exception of storage, only be processed for the purposes of proof, or with the Data Subject's Consent or, where relevant, the Consent of the Data Subject's parent and/or guardian, or for the protection of the rights of another natural or legal person, or where such processing is in the public interest.

11.3.3 Where the processing of Personal Information has been restricted as contemplated in this paragraph 11.3, AEEI must inform the Data Subject before lifting the restriction.

12 RETENTION AND RECORD KEEPING

12.1 The Act requires that AEEI only retains Records for as long as is necessary for achieving the purpose for which the information was collected or subsequently processed, unless –

12.1.1 retention of the Record is required or authorised by law. In this regard the minimum retention schedule attached hereto sets out the various minimum retention periods for certain records prescribed by law;

12.1.2 AEEI reasonably requires the Record for lawful purposes related to its function or activities;

12.1.3 retention of the Record is required by a contract between the parties thereto;

12.1.4 the Data Subject, or his or her parent or legal guardian where relevant, has Consented to the retention of the Record or;

12.1.5 the record is retained for historical, research or statistical purposes provided safeguards are put in place to prevent use for any other purpose.

12.2 Personal Information collected in accordance with paragraph 10 shall be retained –

12.2.1 in the case of Employees for the duration of the Employee's employment and for a period of not more than 7 years thereafter, provided that in the case of information relating to any remuneration including benefits received by former Employees or any information pertaining to pay as you earn or other tax related information, will, if this is in the interest of the former Employee, be retained for an indefinite period;

12.2.2 in the case of Data Subjects who are customers and having regard to any existing or future relationship that AEEI has or may have with such persons, be retained for an indefinite period unless the Data Subject has objected to the retention or otherwise requested a shorter retention period, subject to the provisions of paragraph 12.3 below;

12.2.3 in the case of any other person including applicants for enrolment or employment, for a period of 1 year after receipt of the Personal Information; or

12.2.4 until such Personal Information is superseded, in which case any obsolete Personal Information shall be destroyed.

12.3 Notwithstanding the Data Subject right to object or request a shorter period as contemplated in paragraph 12.2.2 above, this shall not apply to Personal Information and/or information which AEEI is required to retain by law.

12.4 After expiration of the periods contemplated in paragraph 12.1, AEEI shall be required to destroy, delete or de-identify the Record of Personal Information as soon as reasonably possible thereafter provided that AEEI will be entitled to retain Records of Personal Information for periods in excess of those contemplated in paragraph 12.2 above for historical, statistical or research purposes provided that AEEI has established appropriate safeguards against the records being used for any other purpose.

12.5 Any destruction or deletion of a record must be done in a manner that prevents its reconstruction in an intelligible form.

12.6 In instances where AEEI utilises personal information for decision-making purposes, an additional requirement is imposed on AEEI, namely that the records be retained for the period prescribed by law or code of conduct, in the absence of which, for such period which will allow a data subject a reasonable opportunity to access the records.

12.7 Where AEEI receives an objection or request for a shorted retention period from the Data Subject, AEEI shall ensure that such Data Subject's Personal Information

shall be encrypted and access to the encryption key shall be limited to the Information Officer and/or the relevant Deputy Information Officer.

13 SPECIAL PERSONAL INFORMATION

No person shall be entitled to process the Special Personal Information of a Data Subject, unless –

13.1 the Data Subject has provided his or her Consent to the processing of such information;

13.2 where the Data Subject is a child under the age of 18 years of age, the child's parent and/or guardians have provided their Consent to the processing of such information;

13.3 processing is necessary for the establishment, exercise or defence of a right or obligation in law;

13.4 processing is for historical, statistical or research purposes to the extent that –

13.4.1 the purpose serves a public interest and the processing is necessary for the purpose concerned;

13.4.2 it appears to be impossible or would involve a disproportionate effort to ask for Consent;

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

13.4.3 information has deliberately been made public by the Data Subject (and, in the event of the information pertaining to a child (Data Subject under the age of 18 years), such information has been made public with the consent of the parent or guardian of the child); or

13.4.4 the necessary authorisations have been complied with.

PART 3: TRANSBORDER INFORMATION FLOWS

14 TRANSFER OUTSIDE OF SOUTH AFRICA

14.1 Subject to the provisions paragraph 14.2, AEEI, shall not be entitled to transfer the Personal Information of a Data Subject to a third party who does not reside within South Africa.

14.2 Personal Information of a Data Subject may be transferred outside of South Africa where –

14.2.1 the third party concerned is subject to a law, binding corporate rules or a binding agreement which provides an adequate level of protection that –

14.2.1.1 effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of person information relating to a Data Subject who is a natural person and, where applicable, a juristic person; and

14.2.1.2 includes provisions, that are substantially similar to this paragraph 14, relating to the further transfer of Personal Information from the recipient to another third party who is in a foreign country;

14.2.2 the Data Subject (or, where relevant, the Data Subjects' parent and/or guardian) Consents to the transfer;

14.2.3 the transfer is necessary for the performance of a contract between the Data Subject and AEEI, or for the implementation of pre-contractual measures taken in response to the Data Subject's request;

14.2.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between AEEI and a third party; or

14.2.5 the transfer is for the benefit of the Data Subject, and –

14.2.5.1 it is not reasonably practical to obtain the Consent of the Data Subject to that transfer; and

14.2.5.2 if it were reasonably practical to obtain such Consent, the Data Subject would be likely to give it.

14.3 In the event of a transfer of Personal Information as contemplated in this paragraph 14 taking place, the person responsible for such transfer shall be required to

provide the Deputy Information Officer and the Information Officer with details pertaining to the transfer, including but not limited to whether the Consent to the transfer was obtained from the Data Subject and proof of such Consent.

PART 4: DIRECT MARKETING

15 DIRECT MARKETING BY ELECTRONIC COMMUNICATIONS

15.1 The processing of Personal Information of a Data Subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile, SMS or email is prohibited unless the Data Subject (or, where relevant, the Data Subjects parents and/or guardians) –

15.1.1 have given his, her or its Consent to the processing; or

15.1.2 the Data Subject is a Consumers, subject to the provisions of paragraph 15.4 below.

15.2 Prior to sending any direct marketing communication, it must be determined whether the Data Subject has expressly and specifically Consented to receiving such direct marketing communication from AEEI. Where a Data Subject has not provided his, her or its Consent to receiving direct marketing communications from AEEI, no direct marketing communication may be sent to such Data Subject, unless the Data Subject is a customer of AEEI and the provisions contemplated in paragraph 15.4 have been met.

15.3 A Data Subject may only be approached once to obtain his, her or its Consent to receiving direct marketing communications. Should such Consent be refused or withheld by the Data Subject (or, where relevant, the Data Subject's parent and/or guardian), direct marketing communications must not be sent to the Data Subject and the computer information system should clearly indicate the refusal to provide Consent or that no Consent has been obtained from the Data Subject.

15.4 Where the Data Subject is a customer of AEEI, direct marketing communications may only be sent where –

15.4.1 the Personal Information of the customer was obtained in the context of the provision of a service by AEEI to the customer;

15.4.2 the direct marketing communication intended to be sent to the customer must relate to similar services rendered by AEEI; and

15.4.3 the customer (or, where relevant, the customers' parent and/or guardian) has been provided with a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details –

15.4.3.1 at the time when the Personal Information was collected; and

15.4.3.2 on each occasion in which a direct marketing communication is sent to the customer.

15.5 Any direct marketing communication sent to a Data Subject must contain the following information, namely –

15.5.1 details of the identity of the sender or AEEI;

15.5.2 an address or other contact details to which the recipient may send a request that such communications cease; and

15.5.3 an option for the Data Subject to unsubscribe from receiving such direct marketing communications.

PART 5: INFORMATION SECURITY SUPERVISION

16 IMPLEMENTATION OF SECURITY SAFETYGUARDS

16.1 General

16.1.1 AEEI strives to ensure the security, integrity and privacy of personal information submitted. AEEI will review and update its security measures in accordance with future legislation and technological advances. Unfortunately, no data transmission can be guaranteed to be totally secure, however, AEEI will endeavour to take all reasonable steps to protect the Personal Information collected.

16.1.2 AEEI must secure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –

16.1.2.1 loss of, damage to or unauthorised destruction of Personal Information; and

16.1.2.2 unlawful access to or processing of Personal Information.

16.1.3 AEEI has done and will from time to time ensure that it takes reasonable steps to –

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

16.1.3.2 establish and maintain appropriate safeguards against the risks identified;

16.1.3.3 regularly verify that the safeguards are effectively implemented; and

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

16.1.4 In implementing the above measures, AEEI will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

16.2 **Information Security**

16.2.1 AEEI is committed to ensuring information security and in particular ensure that the incidence of unauthorised access to or transmission of Personal Information is minimised.

16.2.2 The following measures have or will be introduced by AEEI and must, where relevant be adhered to -

16.2.2.1 all documents containing Personal Information must be securely stored and access thereto controlled in an appropriate manner. No documentation containing Personal Information must be left unattended or unsecured or otherwise in plain sight or otherwise in an environment with ease of access;

16.2.2.2 all computers and other electronic devices including particularly mobile devices which are capable of storing or accessing data must be secured with passwords which are to be updated on a regular basis;

16.2.2.3 data transmission, such as sending and receiving messages like e-mails must be conducted on, through or by the relevant AEEI information systems provided that this data transmission includes Personal Information. No non AEEI assigned e-mail addresses or non-Company computers or other electronic devices may be used to transmit any Personal Information contemplated herein; and

16.2.2.4 Personal Information should only be saved on the secured network and accordingly, no Personal Information may be saved on any computer local drive or desktop and on other electronic devices.

16.3 **Information processed by Operators**

16.3.1 An Operator or anyone processing Personal Information on behalf of AEEI must –

16.3.1.1 process such information only with the knowledge or authorisation of AEEI; and

16.3.1.2 treat Personal Information which comes to their knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

16.3.2 AEEI shall always ensure that, in terms of a written contract between AEEI and the Operator, the Operator which processes Personal Information for AEEI establishes and maintains the security measures referred to in paragraph 16.1.

16.3.3 The Operator must notify AEEI immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.

16.3.4 Notwithstanding anything to the contrary herein contained, under no circumstances must any Operator be allowed to process any Personal Information unless there is a written contract signed by both parties which deals comprehensively with the matters contemplated in this Policy.

16.4 **Security Compromises**

16.4.1 In the event of there being reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by an unauthorised person and accordingly, resulting in a compromise of the security safeguards of AEEI, the Information Officer upon, notification of such compromise as contemplated in paragraph 8.1.2, shall immediately upon receipt of such notification report same to the Board.

16.4.2 The Information Officer shall be required to notify both the Regulator and the Data Subject concerned within 5 business days of the Board being informed of the compromise as contemplated in paragraph 16.4.1.

16.4.3 The notification to the Data Subject must be in writing and must either –

16.4.3.1 be mailed to the Data Subject's last known physical or postal address; or

16.4.3.2 be sent by email to the Data Subject's last known email address; or

16.4.3.3 be placed in a prominent position on the website of AEEI; or

16.4.3.4 be published in the news media; or

16.4.3.5 as directed by the Regulator.

16.4.4 The notification contemplated in paragraph 16.4.2 must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including –

16.4.4.1 a description of the possible consequences of the security compromise;

16.4.4.2 a description of the measures that AEEI intends to take or has taken to address the security compromise;

16.4.4.3 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

16.4.4.4 if known to AEEI, the identity of the unauthorised third party who may have accessed or acquired the Personal Information.

17 REGULATOR

17.1 The Regulator is a juristic person established in terms of section 39 of the Act. The power, duties and functions of the Regulator are –

17.1.1 to provide education by –

17.1.1.1 promoting an understanding and acceptance of the conditions for the lawful processing of Personal Information and of the objects of those conditions;

17.1.1.2 undertaking education programmes, for the purpose of promoting the protection of Personal Information, on the Regulator's own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator;

17.1.1.3 making public statements in relation to any matter affecting the protection of the Personal Information of a Data Subject or of any class of Data Subjects;

17.1.1.4 giving advice to Data Subjects in the exercise of their rights; and

17.1.1.5 providing advice, upon request or on its own initiative, to a Minister or a public or private body on their obligations under the provisions, and generally on any matter relevant to the operation, of the Act;

17.1.2 to monitor and enforce compliance by –

17.1.2.1 public and private bodies with the provisions of the Act;

17.1.2.2 undertaking research into, and monitoring developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the Personal Information of Data Subjects are minimised, and reporting to the Minister the results of such research and monitoring;

17.1.2.3 examining any proposed legislation, including subordinate legislation, or proposed policy of the Government that the Regulator considers may affect the protection of the Personal Information of Data Subjects, and reporting to the Minister the results of that examination;

17.1.2.4 reporting upon request or on its own accord, to Parliament from time to time on any policy matter affecting the protection of the Personal Information of a Data Subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the Personal Information of a Data Subject;

17.1.2.5 submitting a report to Parliament, within 5 months of the end of its financial year, on all its activities in terms of this Act during that financial year;

17.1.2.6 conducting an assessment, on its own initiative or when requested to do so, of a public or private body, in respect of the processing of Personal Information by that body for the purpose of ascertaining whether or not the information is processed according to the conditions for the lawful processing of Personal Information;

17.1.2.7 monitoring the use of unique identifiers of Data Subjects, and reporting to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the Personal Information of a Data Subject;

17.1.2.8 maintaining, publishing and making available and providing copies of such registers as are prescribed in this Act;

17.1.3 examine any proposed legislation that makes provision for the –

17.1.3.1 collection of Personal Information by any public or private body; or

17.1.3.2 disclosure of Personal Information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44(2), in any case where the Regulator considers that the information might be used for the purposes of an information matching programme;

17.1.4 report to the Minister and Parliament the results of that examination;

17.1.5 to consider with interested parties by –

17.1.5.1 receiving and inviting representations from members of the public on any matter affecting the Personal Information of a Data Subject;

17.1.5.2 co-operating on a national and international basis with other persons and bodies concerned with the protection of Personal Information; and

17.1.5.3 acting as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the Personal Information of a Data Subject;

17.1.6 to handle complaints by –

17.1.6.1 receiving and investigating complaints about alleged violations of the protection of Personal Information of Data Subjects and reporting to complainants in respect of such complaints;

17.1.6.2 gathering such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under the Act;

17.1.6.3 attempting to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation; and

17.1.6.4 serving any notices in terms of the Act and further promoting the resolution of disputes in accordance with the prescripts of the Act;

17.1.7 to conduct research and to report to Parliament –

17.1.7.1 from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the Personal Information of a Data Subject; and

17.1.7.2 on any other matter, including necessary legislative amendments, relating to protection of Personal Information that, in the Regulator's opinion, should be drawn to Parliament's attention;

17.1.8 in respect of codes of conduct to –

17.1.8.1 issue, from time to time, codes of conduct, amend codes and to revoke codes of conduct;

17.1.8.2 make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct; and

17.1.8.3 consider afresh, upon application, determinations by adjudicators under approved codes of conduct;

17.1.8.4 to facilitate cross-border co-operation in the enforcement of privacy laws by participating in any initiative that is aimed as such co-operation; and

17.1.9 in general to –

17.1.9.1 do anything incidental or conducive to the performance of any of the preceding functions;

17.1.9.2 exercise and perform such other functions, powers and duties as are conferred or imposed on the Regulator by or under the Act or any other legislation;

17.1.9.3 require the responsible party to disclose to any person affected by a compromise to the integrity or confidentiality of Personal Information, such compromise in accordance with section 22 of the Act; and

17.1.9.4 exercise the powers conferred upon the Regulator by the Act in matters relating to the access of information as provided by PAIA.

17.2 The contact details of the Regulator may be obtained from the Information Officer during normal working hours.

PART 6: IMPLEMENTATION AND AMENDMENTS

18 DELEGATIONS

No decision making contemplated in this Policy may be delegated to an advisor or consultant of AEEI.

19 AMENDMENTS TO POLICY

19.1 No additions, amendments or deviations from this Policy shall be valid unless approved by the Board.

19.2 Changes or suggestions to amend the Policy shall be done in writing stating the rationale and, where possible, proposed recommendations to amend the Policy. Such recommendations shall be submitted to the Information Officer.

19.3 When deemed necessary in the opinion of the Information Officer and after giving due consideration to the merits and de-merits of the proposals to amend this Policy, the Information Officer shall, where appropriate, submit such recommendations to the Board for its decision. The Board shall thereupon be empowered to accept the proposal or alternatively, accept the proposal subject to conditions that the Board may impose or alternatively, reject the proposal. In making its decision, the Board shall be required to take into consideration the provisions of the Act together with any amendments thereto.

19.4 Where any provision of the Act has been amended, the Board shall be required to convene a meeting to determine whether the aforesaid amendments have an impact on the Policy. Where it is decided that the amendment to the Act has an impact on the Policy, the Board shall be required to amend the Policy to align it with the provisions of the Act as well as the amendments thereto.

20 COMMUNICATION WITH AEEI

20.1 All correspondence with regard to this Policy or any matter arising from or related to the implementation of this Policy, shall be addressed to the Information Officer.

20.2 The Information Officer shall be obliged to inform the Board of any matters of significance in relation to the implementation or otherwise of this Policy.

21 COMBATING ABUSE OF THE POLICY

21.1 The Information Officer shall take all reasonable steps to prevent the abuse of the provisions of this Policy and when justified shall –

21.1.1 take appropriate steps against such official or other role player, provided that such steps shall at all times comply with the relevant laws and processes of AEEI; or

21.1.2 in consultation with the Board may issue a complaint to the Regulator in the manner prescribed by the Act.

21.2 The Information Officer shall inform the Board of any actions taken in terms of this paragraph21.

Annexure "A"

Data Retention Matrix

1. Statutorily prescribed retention periods and regulatory retention periods:

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Accounting / Tax	Finances	Annual/quarterly financial reports, balance sheets, accounts payable, purchase orders, financial and tax related audits, invoices, taxes, audited financial accounts, records relating to reserves, accounting records, expense reports, financial statements, bank accounts and other accounts, inventory, bookkeeping vouchers (e.g. copies of invoices, tax assessments, wage lists, payment instructions, travel expense accounting), risk reports/ models, records of cumulative client assets, source documents to substantiate books of account, returns and reports.	Yes – 5 (Five) years.	Tax Administration Act, No 28 of 2011 ("**TAA**") (Section 29)	For any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act No. 71 of 2008 ("**Companies Act**"), such as annual financial statements, the company is required to keep such records for a period of 7 (seven) years.	N/A	(i) Companies Act - Section 24(1) requires that the information must be kept in written form, or other form or manner that allows that information to be converted into written form within a reasonable time; and (ii) the TAA – Section 30, requires that records be kept a) in their original form in an orderly fashion at a safe place; b) in any other form (including electronic) as may be prescribed by the South Africa Revenue Services ("**SARS**") Commissioner in a public notice; or c) in a form specifically authorised by a senior SARS official.	(i) Companies Act – Section 25, requires records to be accessible at or from the company's registered office or another location within South Africa; (ii) Tax records must be kept in South Africa in order to be available for inspection by a SARS official, per Section 30 of the TAA.	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Corporate Entity	Corporate records	Company Secretarial, certificate of incorporation, title, deeds, board of directors, shareholder records, stock certificates, contracts, agreements, internal/external audit, board minutes, register of shareholders, memorandum and articles of association, register of charges, share transfer documentation, written resolutions, company registers, powers of attorney, annual and quarterly reports, merger treaties, board resolutions, resolutions (i) of stockholder meetings; and/or (ii) regarding amendments to the memorandum of association and related minutes, records on subscriptions to shares, reports of the executive	Yes – As a general rule, for any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act, the company is required to keep such records for a minimum period of 7 (seven) years.	Companies Act, Sections 24 and 85.	(i) Where a company has been in existence for shorter than 7 (seven) years, the company is only required to keep information for that period for which has been in existence (Section 24(2)); (ii) For documents relating to: a) registration certificates; securities registers and uncertificated securities register; register of company secretary and auditors, the company is required to keep such documents indefinitely - (Section 85(1); and b) For real property records such as a title deed, the company is required to keep such documents indefinitely, or until such time that the relevant	N/A	The Companies Act requires that the information must be kept in written form, or other form or manner that allows that information to be converted into written form within a reasonable time.	Companies Act – Section 25(1)(a), requires records to be accessible at or from the company's registered office or another location within South Africa.	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

		board, documentation regarding capital share payments, register of loan agreements between the company and its officers, documents relating to real/ personal property, intellectual property, technical and IT designs/source code/process flows/user documentation and licenses, product documentation, patents, facilities related agreements including supplier agreements, insurance policies and certificates accident records and documentation related to inspections and hazardous materials, fire certificates, pension scheme documents, access control records, security reports, building drawings and plans, building inspections and safety reports business continuity plans.			property is disposed of.				

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Customers and transactions	Records relating to setting up customer accounts and ongoing work with customer including details of transactions entered into by company	Product/service agreements, quotations and order documents, order tracking, order audit trail, statements of work, delivery schedules, terms and conditions, price/volume data, data protection agreements, client advice records, contact details, financial analysis records provided to customer, particulars of each client's assets and liabilities, summaries of telephone conversations relating to orders and transactions, credit records, customer payment , agreements and transactions with third parties other than clients and employees (e.g. suppliers, service providers); Environmental/health and safety policies, claims and records.	Yes – 5 (five) years: (i) in relation to documents relating to establishment of business relations, from the date on which the agreement was terminated; and (ii) in relation to records of transactions concluded, from the date on which the transaction was concluded.	Standard Practice / Financial Intelligence Centre Act, Section 23.	N/A	N/A	Financial Intelligence Centre Act only provides that records kept in terms of sections 22 and 22A may be kept in electronic form but must be capable of being reproduced in a legible format. Where records are kept by a third party on behalf of a company, the company must have free and easy access to the records and the records are readily available to the Centre (per the Financial Intelligence Centre Act - Section 24) and the relevant supervisory body for the purposes of performing its functions in terms of the Financial Intelligence Centre Act.	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Consumer Protection	Records relating to activities performed in an intermediary capacity and records of promotional competitions	Record of information given to the consumer in relation to intermediary activities, written instructions from consumers, terms and conditions of promotional competitions, list of prizes to be awarded, offer to participate.	Yes - 3 (three) years.	The Consumer Protection Act - section 27(3)(b) read with regulation 9 and 10 in relation to an intermediary and section 36 (11)(b) read with regulation 11 in relation to promotional competitions.	N/A	N/A	The Consumer Protection Act – regulation 10(3) provides that records be kept in an appropriate electronic or recorded format, which must be easily accessible and readily reducible to written or printed form.	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Financial Services	Recordings relating to the provision of financial services	Cancellations of transactions by clients of the provider; complaints received; feedback on complaint resolution; statement of non-compliance with Financial Advisory and Intermediary Services Act and reasons therefore; verbal and written communications concerning a financial service rendered.	Yes - 5 (five) years.	The Financial Advisory and Intermediary Services Act - section 18 and the General Code of Conduct for Authorised Financial Services Providers and Representatives ("**the Code**") – Section 3.	Only in so far as the financial service provider has been exempt of its document retention obligations by the Registrar.	N/A	Financial Advisory and Intermediary Services Act provides that records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form and the Code provides that providers are not required to keep the records themselves but must ensure that they are available for inspection within 7 (seven) days of the registrar's request. Records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form.	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Employees and HR	Records relating to employees	Employee records and payroll, personnel files, job applications, work authorisations, pension, CVs, background checks, licenses / reviews / examinations, training records, personal dealing, injuries/accidents, health and safety, employee contracts, personnel records (including director's investment policy), records of benefits, disability records, unsuccessful applications, expense records, pension and investment policy, temporary employee contracts, attendance records, profit sharing agreements, medical files, test papers, references, job descriptions, employment passes/visas/work permits, drug testing and interview notes.	Yes – 3 (three) years	Basic Conditions of Employment Act No 75 of 1997 ("**BCEA**") – Section 29(4) and Section 31; and Labour Relations Act 66 of 1995 ("**LRA**") – Section 205(1) – (2) and Section 205(3) read with Schedule 8 – Section 5	(i) The Compensation for Occupational Injuries and Diseases Act 130 of 1993 ("**COIDA**"), Section 81(1) and (2), requires employers to retain the following information for a period of 4 (four) years from the date of last entry into the relevant record: a) register, record or reproduction of the earnings, b) time worked, c) payment for piece work and overtime and d) other prescribed particulars of all the employees; (ii) The Occupational Health and Safety Act 85 of 1993 -Section 20(2), under the following Regulations: Asbestos Regulations, 2001, Regulation 16(e) and (f), Hazardous	N/A	N/A	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

					Biological Agents Regulations, 2001, Regulation 9(1) and (2); Hazardous Chemical Substance Regulations, 1995, Regulation 9; Lead regulations, 2001, Regulation 10; and Noise Regulations, Regulation 11, requires certain information to be kept for 30 – 40 (thirty to forty) years. Other exceptions include that staff records (after employment terminated) are to be retained for 7 (seven) years (per BCEA and COIDA); time and piecework records are to be retained for 7 (seven) years (per BCEA and COIDA); UIF contributor's cards are to be retained until service is terminated (per BCEA -Section 29(4) and per Unemployment Insurance Act, No 63 of 2002 – Section 56(2)(c)) and wage and salary records (including overtime) should be retained for 7 (seven) years (per TAA, BCEA				

					and COIDA). In respect of payroll and wage records, details of overtime worked, bonuses, expenses and benefits in kind, given their potential relevance to pay disputes they should be retained for seven years after employment ends (standard practice – a longer retention period is therefore prescribed). LRA, Section 205(3) – requires employers to retain prescribed details of any strike, lock-out or protest action involving its employees Indefinitely.				

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Legal / Regulatory	Required reports to regulatory enquiries	Regulatory submissions, legal/regulatory enquiry, investigation, complaints, lawsuits, subpoenas, hearings, litigation files, legal correspondence. records of regulatory relationships, records relating to management of pension scheme, details of risk management systems, documents relating to tax investigation, financial promotion records, records of lending policy, fraud reports to regulators, money laundering reports, Insurance claims, compliance records including reports & fillings,	No – Indefinitely	N/A	N/A	Standard Practice	Not specified	Not specified	

		regulatory audit reports, succession files, records required to demonstrate compliance with regulatory requirements, internal organisation schemes, records on internal control systems, records on internal audits, reports to management, IT-emergency documents, records on information on private and corporate customers and transactions (with regard to money laundering and insider trading).							
General	Correspondence and publications (to the extent not addressed above)	General correspondence (electronic or otherwise), press releases, publications.	3 (three) years	Standard Practice	N/A	Subject to certain exceptions, a civil claim may be brought against a company for a period of up to 3 years in South Africa (because the general prescription period in South Africa is 3 years)	N/A	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

2. Standard practice retention periods

The retention periods below apply generally to the extent that there are no statutorily prescribed retention periods or regulatory periods. Accordingly, the following guideline retention periods are standard practice of the Company.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Standard practice retention period	Exceptions to retention periods	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Employment related	Recruitment records (pre-employment)	Completed online application forms or CVs; Equal opportunities monitoring forms; Assessment exercises or tests; Notes from interviews and short-listing exercises; Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references; Criminal records checks.	For unsuccessful candidates 6 (six) – 12 (twelve) months after notifying candidates of the outcome of the recruitment exercise. These records may be transferred to a successful candidate's personnel file if they are relevant to the ongoing employment relationship.	Only in so far as the BCEA or LRA retention periods do not apply to the relevant records.	N/A	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Standard practice retention period	Exceptions to retention periods	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Employment related	Collective agreements	Any copy of a relevant collective agreement, collective workforce agreements and past retained on an employee's record will remain while agreements that could affect present employees.	While employment continues and for seven years after the contract ends.	Only in so far as the BCEA or LRA retention periods do not apply to the relevant records.	N/A	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Standard practice retention period	Exceptions to retention periods	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Client records	Client records – Contracts	Any contracts with clients.	These documents must be kept for a period of at least 5 (five) years after the cancellation of the contract.	N/A	N/A	N/A	An external service provider to destroy documents and IT to delete information from all systems including servers, cloud storage and laptops and all electronic devices.

Adopted and approved by the Board of Directors on 28 July 2021