AMARI PROPERTY MANAGEMENT

PROTECTION OF PERSONAL INFORMATION ACT MANUAL

1. CONTENTS

2. DEFINITIONS

1.1	**DATA SUBJECT**	means the person to whom personal information relates to.
1.2	**FURTHER PROCESSING**	means processing personal information for a process other than what it was initially collected for.
1.3	**GROSS NEGLIGENCE**	means a conscious, voluntary act or omission in the reckless disregard of a legal duty to keep personal information safe and therefore at the consequence of another.
1.4	**HEAD**	in relation to the Association means the Chairman of the Board of Trustees or Directors.
1.5	**INFORMATION OFFICER**	means the person who is responsible for ensuring the Association's compliance with POPIA. The Chairperson of the Association is elected as the designated Information Officer. The Information Officer must be registered with the South African Information Regulator that has been established under POPIA prior to the commencement of his/her duties. The Association may elect a Deputy Information Officer to assist the Information Officer with his/her duties.
1.6	**PAIA**	means the Promotion of Access to Information Act 2 of 2000.
1.7	**PERSON**	means a natural person or a juristic person.
1.8	**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: a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing,

		disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d) the biometric information of the person; e) the personal opinions, views or preferences of the person; f) 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; g) the views or opinions of another individual about the person and; h) 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.
1.9		
1.10		
1.11	**PERSONAL REQUESTER**	means a requester seeking access to a record containing Personal Information about the requester.
1.12	**POPIA**	refers to the Protection of Personal Information Act 4 of 2013.
1.13	**PRIVATE BODY**	Means a natural person who carries or has carried on any trade, business or profession, but only in such capacity, a partnership which carries or has carried on any trade, business or profession or any former or existing juristic person, but excludes a public body.

1.14	**PUBLIC BODY**	means a natural person who carries or has carried on any trade, business or profession, but only in such capacity, a partnership which carries or has carried on any trade, business or profession or any former or existing juristic person, but excludes a public body.
1.15	**PUBLIC RECORD**	means a record that is accessible in the public domain and which is in the possession of or under control of a public body, whether or not it was created by a public body.
1.16	**RECORD**	means any recorded information- a) regardless of form or medium, including any of the following; (i) writing of any material; (ii) 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; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) 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; b) in the possession or under the control of a responsible party; c) whether or not it was created by a responsible party; and d) regardless of when it came into existence.
1.17	**RESPONSIBLE PARTY**	means a public or private body or any other person which, alone or in conjunction with others determines the

		purpose of and means for processing personal information.
1.18	**REQUESTER**	in relation to the Association means any person, including, but not limited to a public body or an official thereof, making a request for access to a record of the Association or a person acting on behalf of such a person.
1.19	**REQUEST FOR ACCESS**	means a request for access to a record of the Association in terms of section 50 of PAIA.
1.20	**THE ASSOCIATION**	means Amari Property Management and all Trustees and / or Managing Agents who are responsible for the storage, processing, protection and destruction of all Personal Information.
1.21	**THIRD PARTY**	in relation to a request for access to a record held by the Association, means any person other than the requester.
1.22	**WILFUL MISMANAGEMENT**	means intentionally managing personal information without care and wrongfulness.

3. PURPOSE

3.1 The primary purpose of this policy is to provide guidance to members of the Association with regards to the requirements and guidelines of processing and storing data subject's personal information.

3.2 The Association will therefore ensure that each and every Member of the Association is aware of the manner in which their Personal Data is handled / stored and destroyed as well as retained as per the requirements by law.

3.3 This policy will also provide guidance to Trustees as they carry out their duties in accordance with the guidelines and performances stated in this policy as well as within the ambient of the guidelines and procedures of the Protection of Personal Information Act.

3.4 This document will therefore be of assistance in regulating the primary functionalities of balancing the right to privacy and the right to access of information. This policy will further assist the Association to establish and understand the conditions that must be adhered to when processing and storing Members or any Tenant's personal information.

4. SCOPE AND OBJECTIVE OF THE POLICY

This policy is applicable to all Trustees and Members of the Association, including all Service Providers, Contractors and Employees that have access to Members or Tenants information.

5. RIGHTS OF DATA SUBJECTS

5.1 A Data Subject has the right to have his / her / its personal information processed in accordance with the conditions with POPIA, which rights includes:

5.1.1 To establish whether a responsible party holds personal information of a data subject;
5.1.2 To request access to his / her / its personal information;
5.1.3 To request, where necessary, the correction, destruction or deletion of his / her / its personal information;
5.1.4 To object, on reasonable grounds that relates to his / her / its particular situation to the processing of his / her / its personal information that has been provided;
5.1.5 To object to the processing of his / her or its personal information being used for purposes of direct marketing or direct marketing by means of unsolicited electronic communications.
5.1.6 To not have his, her or its personal information for purposes of direct marketing by means on unsolicited electronic communications;
5.1.7 To not be subject, under certain circumstance, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person;
5.1.8 To submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in the Act; and
5.1.9 To institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

POPI is implemented by abiding by eight processing conditions. The Association shall abide by these principles in all its processing activities.

In summary to the above, a Data Subject has the right to know when their personal information is being collected, to be told when someone requests their personal information and whether they have the right to collect your information. To request that their information be deleted or amended, to object to having their information processed for marketing purposes and to object against automation of information with the intent to provide a profile, to submit complaints / grievances.

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

POPI is implemented by abiding by eight processing conditions. The Body Corporate shall abide by these principles in all its processing activities.

6. ACCOUNTABILITY

6.1 The Association are to ensure that personal information is lawfully processed in accordance with POPI Act at all times.
6.2 As the responsible party, the Association is required to audit the processes used to collect, record, store, disseminate and destroy personal information. The Association is to ensure

the integrity and safekeeping of personal information that is in its possession or under its control.

6.3 The Association must take steps to prevent date subject's information from being lost, damaged or unlawfully accessed by storing the personal information in a manner that will not be accessible to unauthorised parties.

6.4 The Association must ensure that all processing conditions in terms of POPI are complied with when determining the purpose and means of processing Personal Information.

7. PROCESSING LIMITATION

Personal information may only be processed in a fair and lawful manner and only with the consent of the data subject.

7.1 Lawfulness of processing:

7.1.1 Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

7.1.2 Processing is deemed to be lawful only when a purpose is given, the information obtained is adequate and that the information obtaining is relevant and not excessive.

7.1.3 Personal Information may only be processed by the Association if one of the following grounds of lawful processing exists:

7.1.3.1 The Data Subject consents to the processing of their personal information;

7.1.3.2 Processing is necessary for the conclusion or performance of a contract with the Data Subject, including but not limited to the below:

7.1.3.2.1 Arranging for maintenance in units;

7.1.3.2.2 Security control and access control (including but not limited to CCTV footage and biometric data);

7.1.3.2.3 Financial information;

7.1.3.2.4 Association Employees; and

7.1.3.2.5 Receive communication from the Association when / if needed.

7.1.3.2.6 Processing complies with a legal responsibility imposed on the Association (should the Association be privy to any legal proceedings or obligations as imposed by the law;

7.1.3.2.7 Processing protects a legitimate interest of the Data Subject;

7.1.3.2.8 Processing is necessary for pursuance of a legitimate interest of the Association; and

7.1.3.2.9 Data subject consent is not required if it would prejudice a lawful process or if the information is contained in a public record.

7.2 Special Personal Information includes:

7.2.1 Religious, philosophical or political beliefs;

7.2.2 Race or ethnic origin;

7.2.3 Trade union membership;

7.2.4 Health status or sex life;

7.2.5 Biometric information (including but not limited to: blood type, fingerprints, DNA, retinal scanning, voice recognitions, photographs);

7.2.6 Criminal behaviour;

7.2.7 Information concerning a child.

7.3 The Association may only process Special Personal Information under the following circumstances:

7.3.1 The Data Subject has consented to such processing;

7.3.2 The Special Personal Information was deliberately made public by the Data Subject;

7.3.3 Processing is necessary for the establishment of a right or defence in law;

7.3.4 Processing is for historical, statistical or research reasons; and / or

7.4 All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object at any time to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data Subject withdraws consent or objects to processing then the Association, shall immediately refrain from processing the Personal Information.

8. PURPOSE SPECIFICATION

Personal information may only be processed for a specific, explicitly defined and legitimate reason. Personal information may not be processed for any other reason besides the reason it was obtained for, e.g., communication with owners and tenants.

8.1 Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity that the Association renders.

8.2 The Association is to ensure that the Data Subjects are aware of the purpose for the collection of the information that is being obtained.

8.3 The purposes for collecting Data Subjects Personal Information must remain within the ambient of the following:

8.3.1 Administration of agreements;

8.3.2 General security – including but not limited to CCTV footage, biometric access;

8.3.3 Security incidents; general member / resident communication;

8.3.4 Access control;

8.3.5 Financial management;

8.3.6 Arranging of maintenance;

8.3.7 Marketing and sales;

8.3.8 In connection with any legal proceedings;

8.3.9 Staff administration;

8.3.10 Keeping of accounts and records;

8.3.11 Financial management – including but not limited to the keeping of financial information of accounts in arrears;

8.3.12 Access to the facilities in the Association;

8.3.13 Complying with legal and regulatory requirements; and

8.3.14 Any transactions that are incidental to the operations of the Association.

8.4 Retention and Restriction of Records:

8.4.1 Subject to the above and Annexure A of this policy, records of Personal Information must not be kept longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.

8.4.2 Once the time periods have lapsed set out in Annexure A, the Association must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the Association is no longer authorised to retain the record in terms of Annexure A.

8.4.3 The Association must ensure that the destruction or deletion of Personal Information must be done in a manner that prevents its reconstruction in an intelligible form.

9. FURTHER PROCESSING LIMITATION

Personal information may not be processed for a secondary purpose unless the processing is compatible with the original purpose. Should you require to use the data subject's personal information for a reason other than what it was collected for, you will need to obtain consent, again, from the data subject before you can make use of their personal information.

E.g., if you intend to reuse personal information, is it in accordance and compatible with the purpose for which it was collected for?

9.1 Further processing of Personal Information must be in accordance with or compatible with the purpose for which it was collected in its specific purpose.

9.2 Further processing is necessary in the following instances:

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

9.2.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

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

9.2.4 Is the interest of national security.

9.3 In order to assess if further processing is compatible with the purpose of collection, the Association must take into account the following:

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

9.3.2 The nature of the information concerned;

9.3.3 The consequences of the intended further processing for the date subject;

9.3.4 The manner in which the information has been collected; and

9.3.5 Any contractual rights and obligations between the parties.

9.4 Further processing of Personal Information is incompatible with the purpose of collection if:

9.4.1 The Data Subject or a competent person where the Data Subject is a child has consented to the further processing of the information;

9.4.2 The information is available in or derived from a public record or has been deliberately made public by the data subject.

10. INFORMATION QUALITY

The Body Corporate must ensure that the information obtained is not incorrect in any way.

10.1 The Association must take reasonable steps to ensure that the Personal Information obtained from Data Subjects is complete, accurate, not misleading and updated where necessary.

10.2 By taking the steps referred to in 9.1, Trustees and Managing Agents of the Association must have regard to the purpose for which Personal Information is collected or further processed.

10.3 All authorised persons should as far as reasonably practicably follow the following guidance when collecting Personal Information:

10.3.1 Personal Information should be dated when received;

10.3.2 A record should be kept of where the Personal Information was obtained;

10.3.3 Changes to information records should be dated;

10.3.4 Irrelevant or unneeded Personal Information should be deleted or destroyed;

10.3.5 Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system or both.

11. OPENNESS

The Body Corporate must ensure that the data subject is aware that their personal information is being collected and for what purpose their personal information will be used for.

11.1 The Association must maintain the documentation of all processing operations under its responsibility as referred under retention and restriction of records.

11.2 The Association must take reasonable practical steps to ensure that the Data Subjects are aware of:

11.2.1 The information being collected and where the information is not collected from the data subject, the source from which it is collected;

11.2.2 The persons in charge of handling personal data within the Association;

11.2.3 The purpose for which the information is being collected;

11.2.4 Whether or not the supply of the information by that data subject is voluntary or mandatory;

11.2.5 The consequences of failure to provide the information;

11.2.6 Any particular law authorising or requiring the collection of the information;

11.2.7 The fact that, where applicable, if the Association intends to share the information to a third party or international organisation and the level of protection afforded to the information by that third party or international organisation;

11.2.8 That the Data Subject has the right to access or rectify the information collected;

11.2.9 That the Data Subject has the right to object to the processing of their Personal Information; and

11.2.10 The Association have the obligation to inform the Data Subject that should they be unhappy in the manner in which their Personal Information is being processed or stored that they have the right to lodge a complaint to the Information Regulator.

11.3 Minutes recording during meetings must be stored in a safe facility where it cannot be accessed by unauthorised persons by one designated Trustee/Director.

12. SECURITY SAFEGUARDS

Personal information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorised destruction and disclosure.

12.1 The Association must ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

12.1.1 Identify all reasonably foreseeable risks to information security; and

12.1.2 Establish and maintain appropriate safeguards against such risks.

12.2 Written records:

12.2.1 Personable Information records should be kept in locked cabinets or safes by an elected the appointed Managing Agent or designated Trustee should no Managing Agent be appointed, who has been designated to keep the Personal Information;

12.2.2 Minute Books should be kept with the appointed Managing Agent or designated Trustee should not Managing Agent be appointed, mentioned above;

12.2.3 When in use, Personal Information records should not be left unattended in areas where non-members may access these;

12.2.4 The Association shall designate the appointed Managing Agent or designated Trustee should no Managing Agent be appointed to physically (if necessary) store any personal information of member or their tenants; and

12.2.5 Personal Information which is no longer required should be disposed by shredding or in a manner where it cannot be reconstructed.

12.3 Any loss, theft or unauthorised access to Personal Information must be immediately reported to the Information Officer.

12.4 Electronic Records:

12.4.1 All electronically held Personal Information must be saved on an online server / Cloud;

12.4.2 Only authorised Trustees will have access to this online server / Cloud;

12.4.3 All computers, laptops and hand-held devices should be access protected with a password, fingerprint, retina scan or facial recognition, with the password being of reasonable complexity and changed monthly;

12.4.4 The Association shall implement an online portal where electronic copies of minutes taken from meetings are stored and only authorised persons are allowed access to same; and

12.4.5 Electronic Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employees must ensure that the information has been completely deleted and is not recoverable.

12.5 Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer who shall notify the appointed Managing Agent who is the in charge of the online storage of Personal Information and who will ensure that the information is permanently deleted. The Association must make use of an IT service who will ensure that the Personal Data that was stored on the device has been remotely deleted.

13. DATA SUBJECT PARTICIPATION

Data subjects may request that their personal information amended or destroyed.

13.1 Data Subjects have the right to request access to, amendment or deletion of their Personal Information.

13.2 All such requests must be submitted in writing to the Information Officer, unless there are grounds for refusal as set out in paragraph 16.3. The Association shall disclose the requested Personal Information:

13.2.1 On receipt of adequate proof of identity from the Data Subject or requestor;

13.2.2 Within a reasonable time;

13.2.3 On receipt of the prescribed fee, if any;

13.2.4 In a reasonable format.

14. CATEGORIES OF RECIPIENTS FOR PROCESSING PERSONAL INFORMATION

14.1 The Association may share Personal Information with its contractors who attend to the maintenance and upkeep of any asset or aspect of the Association, if Personal Information is required.

14.2 The Association may share Personal Information with Employees of the Association should it be necessary to do so.

14.3 The Association may share Personal Information for general security purposes, security incidents, general member / resident communication and financial management.

15. RETENTION OF PERSONAL INFORMATION OF RECORDS

15.1 The Association may not retain personal information records indefinitely, unless the Data Subject agrees thereto. Personal Information that is in the possession of the Association shall retain the Personal Information records to the extent permitted or required by law. See Annexure “A”.

15.2 The Association is required to delete and destroy any Personal Information that is held about a member or his/her/its tenant once they move out.

16. GENERAL DESCRIPTION OF INFORMATIONS SECURITY MEASURES

16.1 The Association employs up to date technology to ensure the confidentially, integrity and availability of the Personal Information under its case. These measures include:

16.1.1 Firewalls;

16.1.2 Virus protection software and updated protocols;

16.1.3 Logical and physical access control;

16.1.4 Secure setup of hardware and software making up the IT infrastructure;

16.1.5 Outsourced Service Providers who process Personal Information on behalf of the Association are contracted to implement security controls.

17. ACCESS TO PERSONAL INFORMATION

17.1 All individuals and entities may request access, amendment or deletion of their own Personal Information held by the Association. Any requests should be directed, on the prescribed form (REQUEST FOR ACCESS TO RECORD – See Annexure B) to the Information Officer.

17.2 Remedies available if request for access to Personal Information is refused:

17.2.1 Internal Remedies:

The Act does not provide any internal remedies should a request for Personal Information is made and is denied by the Information Officer. As such, the requestor must exercise external remedies at their disposal.

17.2.2 External Remedies:

Should a requestor or third party be dissatisfied with the Information Officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

17.3 An Information Officer may refuse the request to Personal Information on the following grounds:

17.3.1 If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;

17.3.2 If disclosure of the record would endanger the life or physical safety of an individual;

17.3.3 If disclosure of the record would prejudice or impair the security or property or means of transport;

17.3.4 If disclosure of the record would prejudice or impart the protection of the safety of the public;

17.3.5 The record is privileged from production in legal proceedings, unless the legal privilege has been waived; and

17.3.6 Disclosure of the record (containing trade secrets, financial, commercial or technical information) would harm the commercial or financial interest of the Association.

17.4 Records that cannot be found or do not exist:

17.4.1 Should a Data Subject request the Association to search for a record and it is believed that the record does not exist or cannot be found, the requestor must be notified by way of affidavit or letter by the Association. Steps that were taken to try locate this record must be stated on the affidavit / letter.

18. IMPLEMENTATION GUIDELINES

18.1 TRAINING AND DISSEMINATION OF INFORMATION

18.1.1 This Policy has been sent to all members within the Association who are responsible for ensuring that their tenants receive same, as POPI will affect employees, trustees, managing agents, contractors, security personnel or any other party who is required to fulfil any other role in relation to the Association.

18.1.2 All new employees will be made aware of this policy or through training programmes of their responsibilities under the terms of this Policy and POPI Act.

18.1.3 Modifications and updates to data protection and information sharing policies, legislation or guidelines will be brought to the attention of all staff.

18.2 EMPLOYEE CONTRACTS

18.2.1 Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information and a confidentiality undertaking that the employee will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information that the employee deals with or is in charge of, however it is stored. Failure to comply will result in the necessary disciplinary action being taken against the contravening employee.

18.2.2 Each employee who is currently employed with the Association will sign an addendum to their Employment Contact containing the relevant consent clauses for the use and storage of employee information and a confidentiality undertaking that the employee will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information that the employee deals with or is in charge of, however it is stored. Failure to comply will result in the necessary disciplinary action being taken against the contravening employee.

18.3 MEMBERS RESPONSIBILITY

18.3.1 All members of the Association must acknowledge receipt of this manual and ensure that their tenants have received same by acknowledging receipt of this manual and consenting to their Personal Data being stored by the Association.

19. DIRECT MARKETING

19.1 All Direct Marketing communications shall contain an option for the member to opt-out or receiving further marketing communication.

19.2 Existing members:

19.2.1 Direct Marketing by electronic means to existing members is only permitted:

19.2.1.1 If the member`s details were obtained in the context of a service; and

19.2.1.2 For the purpose of marketing similar products or content.

19.2.2 A member must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

19.3 Consent

19.3.1 The Association may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it.

19.4 The Association shall keep record of:

19.4.1 Date of consent;

19.4.2 Wording of the consent;

19.4.3 Who obtained the consent;

19.4.4 Proof of opportunity to opt-out on each marketing contact;

19.4.5 Record of opt-outs.

20. DESTRUCTION OF DOCUMENTS

20.1 Documents may be destroyed after the termination of the retention period specified in Annexure "A" or as determined by the Association from time to time.

20.2 The documents must be shredded so that it will be incapable of being reconstructed.

20.3 Deletion of electronic records must be done in consultation with the IT Service, to ensure that deleted information is incapable of being reconstructed and / or recovered.

21. INFORMATION OFFICER

21.1 The Association will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

21.2 The Information Officer is responsible for ensuring compliance with POPI Act.

21.3 The Association may annually consider a change in the Information Officer and Deputy Officer.

21.4 The Information Officer will be issued with Guidance Notes on their duties and same can be accessed on request to the Information Officer (See Clause 6 of the Guidance Notes).

21.5 The Information Officer is to attend to any complaints issued to him / her on the prescribed form – see Annexure "C".

22. DISCIPLINARY ACTION

22.1 Where a POPI Act compliant or investigation has been finalised, the Association may recommend any appropriate administrative, legal and / or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

22.2 In the case of ignorance or minor negligence, the Association will undertake to provide further awareness training to the employees.

22.3 Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct which may result in summarily dismissal of the employee responsible.

22.4 Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

23. INFORMATION TECHNOLOGY

23.1 The Association must ensure that their IT infrastructure adheres to:

23.1.1 Ensuring that the IT infrastructure, electronic filing system and any other devise used for processing personal information meet acceptable security standards.

23.1.2 ensuring that all electronically held personal information is kept only on designated drives and serves and are uploaded only to approved cloud computing services.

23.1.3 Ensuring that all servers containing personal information are stored in a secure location, away from the general office space.

23.1.4 Ensuring that all back-ups containing personal information are protected from unauthorised access and malicious hacking attempts.

24. EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF THE ASSOCIATION

24.1 All employees and other persons acting on behalf of the Association will, during the course of the scope and duties of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

24.2 Employees and other persons acting on behalf the Association are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

24.3 Employees and other persons acting on behalf of the Association may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Association or externally, any personal information, unless such information is already publicly known or the disclosure thereof is necessary in order for the employee or person to perform his or her duties.

24.4 Employees and other persons acting on behalf of the Association must request assistance from the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

24.5 Employees and other persons acting on behalf of the Association must adhere to the 8 processing conditions of personal information at all times and must always obtain consent from the Data Subject before processing / using or storing their Personal Information.

Annexure "A"

Legislation	Document Type	Period
Companies Act	• Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; • Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; • Copies of reports presented at the annual general meeting of the company; • Copies of annual financial statements required by the Act; • Copies of accounting records as required by the Act; • Record of directors and past directors, after the director has retired from the company; • Written communication to holders of securities and • Minutes and resolutions of directors' meetings, audit committee and directors' committees. • Registration certificate; • Memorandum of Incorporation and alterations and amendments; • Rules; • Securities register and uncertified securities register; • Register of company secretary and auditors and • Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	6 Years Indefinitely
Consumer Protection Act	• Full names, physical address, postal address and contact details; • ID number and registration number; • Contact details of public officer in case of a juristic person; • Service rendered; • Cost to be recovered from the consumer; • Frequency of accounting to the consumer; • Amounts, sums, values, charges, fees, remuneration specified in monetary terms;	3 Years

	• Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;	
Financial Intelligence Centre Act	• Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; • If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; • If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; • The manner in which the identity of the persons referred to above was established; The nature of that business relationship or transaction; • In the case of a transaction, the amount involved and the parties to that transaction; • All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; • The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; • Any document or copy of a document obtained by the accountable institution	5 Years
Compensation for Occupational Injuries and Diseases Act	• Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees. • Section 20(2) documents: -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; -Records of incidents reported at work.	4 Years 3 Years
Basic Conditions of Employment Act	• Section 29(4): -Written particulars of an employee after termination of employment; • Section 31: -Employee's name and occupation; -Time worked by each employee; -Remuneration paid to each employee; -Date of birth of any employee under the age of 18 years. 3 years Employment Equity Act.	3 Years

Employment Equity Act	• Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; • Section 21 report which is sent to the Director General.	3 Years
Labour Relations Act	• Records to be retained by the employer are the collective agreements and arbitration awards. 3 years • An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; • Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employee and the reasons for the actions.	3 Years Indefinite
Unemployment Insurance Act	• Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.	5 Years
Tax Administration Act	• Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -Will enable SARS to be satisfied that the person has observed these requirements	5 Years
Income Tax Act	• Amount of remuneration paid or due by him to the employee; • The amount of employee's tax deducted or withheld from the remuneration paid or due; • The income tax reference number of that employee; • Any further prescribed information; • Employer Reconciliation return.	5 Years
Value Added Tax Act	• Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; • Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; • Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; • Documentary proof substantiating the zero rating of supplies;	5 Years

	• Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	
Sectional Titles Scheme and Management Act	• Account details, contact details, name and surname, ID numbers.	Once member / tenant moves out, any personal information that is not stated above must be deleted and destroyed.

Annexure "B"

PERSONAL INFORMATION REQUEST FORM
Please submit the completed form to the Information Officer

Please be aware that we may request you to provide proof of identification prior to processing your request.
There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject:	
Name & Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
E-mail Address:	

B. Request:
I request the company to (please circle the relevant request(s)): **a. Inform me whether it holds any of my personal information.** **b. Provide me with a record or description of my personal information.** **c. Provide me with a record or description of my personal information.** **d. Correct or update my personal information.** **e. Destroy or delete a record of my personal information.**

C. Instructions:

D. Signature and date:
_____ _____

Annexure "C"

POPIA COMPLAINT FORM
We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer:

Name	
Contact Number	
E-mail Address	

Where we are unable to resolve your complaint to your satisfaction you have the right to lodge a complaint with the Information Regulator.

The Information Regulator: **Advocate Pansy Tlakula**
Physical Address: **SALU Building, 316 Thabi Sehume Street, Pretoria**
E-mail Address: **inforreg@justice.gov.za**
Website: **http://www.justice.gov.za/inforeg/index.html**

A. Particulars of Complaint:	
Name & Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
E-mail Address:	
B. Details of Complaint:	
C. Desired Outcome:	