



**CODE OF CONDUCT
(POPIA)**

**CODE OF CONDUCT GOVERNING
THE CONDITIONS FOR LAWFUL
PROCESSING OF PERSONAL INFORMATION BY
WILLOW ACRES ESTATE**

Registration No.: 2003/018683/08

**ISSUED IN TERMS OF SECTION 60 OF THE PROTECTION
OF PERSONAL INFORMATION ACT, NO. 4 OF 2013
("POPIA") BY THE INFORMATION REGULATOR.**

TABLE OF CONTENTS

	Page Number
PART A – INTRODUCTION	4
1. Background of the Company	4
2. Company Code of Conduct (PoPIA)	4
3. Mandate and Application	5
4. Purpose	5
5. Scope	5
6. Definitions and Abbreviations	6
7. Part B of this Code of Conduct Deals with Each of:	12
7.1 The lawful conditions for processing of personal information	12
7.2 The processing of special personal information, and	12
7.3 The processing of personal information of children	12
8. The Duties and Responsibilities of the Information Officer:	12
9. Commencement of the Code	12
PART B – CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION	14
10. General	14
11. Condition 1: Accountability	15
12. Condition 2: Processing Limitation	16
13. Condition 3: Purpose Specification	18
14. Condition 4: Further Processing Limitation	22
15. Condition 5: Information Quality	23
16. Condition 6: Openness	23
17. Condition 7: Security Safeguards	25
18. Condition 8: Data Subject Participation	32
19. Processing of Special Personal Information	35
20. Processing Of Personal Information of Children	35
21. Disclosure of Personal Information	36
22. Access and Correction of Personal Information	37
23. Amendments to this code	37
24. Notification of Security Compromises	37
25. Other Applicable Legislation	38
PART C - ACTS, POLICIES AND PROCEDURES	39
26. Retention and Confidentiality of documents, information and electronic transactions	39
27. Access to documents	40
28. Disclosure to 3rd Parties	40
29. Storage of Documents	41
29.1 Hard Copies	41
29.2 Electronic Video Recordings / Security Video footage	41
29.3 Minimum Period of retention	49
29.4 Maximum Period of Retention	49
29.5 The Electronic Communications Act	50
29.6 Electronic Record Keeping obligations in terms of other legislations	51
29.7 Preserving the integrity of original electronic records and ensuring that electronic copies accurately represent the original	51

29.8	Companies Act	53
29.9	Basic Conditions of Employment Act 75 of 1997	62
29.10	Compensation for Occupational injuries and diseases act 130 of 1993	66
29.11	Labour Relations Act 66 of 1993	68
29.12	Unemployment Insurance Act No 63 of 2002	73
29.13	Electronic Storage	74
29.14	Destruction of documents	74
29.15	Shredding Policy	75
PART D – INFORMATION OFFICER, DIRECT MARKETING AND TRANSBORDER INFORMATION FLOWS		76
30.	Information Officer	76
31.	Company Appointed Information Officers	76
32.	Direct Marketing by Means of Unsolicited Electronic Communication and Automated Decision-Making	79
33.	Transborder Information Flows	83
PART E – ENFORCEMENT		85
34.	Interpretation of PoPIA and this Code of Conduct	85
PART F – ADMINISTRATION OF CODE OF CONDUCT		86
35.	Compliance with Chapter 7 of PoPIA	86
36.	SOURCES	89
37.	APPENDIXES	90

PART A – INTRODUCTION

1. BACKGROUND OF THE COMPANY

The COMPANY is a Homeowners Association of a residential estate and a non-profit company as defined in the Companies Act No. 71 of 2008; that protects the rights of all of its members residing at the Willow Acres Estate; collects its levies, including ancillary charges and runs the common areas of the Estate. In the provision of Community Services (Levy, maintenance of common property, provision of access & security services) to its members (home owners and residents within the gated community known as Willow Acres Estate), the COMPANY makes use of information that identifies or relates specifically to natural persons (home owners, contractual tenants, visitors, contractors, domestic workers and other service providers) including but not limited to financial information, name, age, identity number, assets and liabilities, income and payment records (Personal Information), biometric information (fingerprints), CCTV footage and Speed Sentry recordings. Broadly, the COMPANY, in the provision of the service to its members and tenants, collects, collates, modifies, stores and distributes the Personal Information of such natural persons, (collectively referred to as "Processing").

PoPIA requires the COMPANY to inform its members, their visitors and employees as to the manner in which their personal information is used, disclosed and destroyed.

The COMPANY is committed to protecting its members, their visitors and employee's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

This code of conduct sets out the manner in which the WAHOA deals with their members, their visitors and employees' personal information as well as and stipulates the purpose for which said information is used. The Code of Conduct is made available on the WAHOA website www.willowacres.co.za and by request from the WAHOA office.

2. COMPANY CODE OF CONDUCT (POPIA)

2.1 "Enforcement" in Chapter 10 and "Offences, Penalties and Administrative Fines" in Chapter 11 of PoPIA.

2.2 The COMPANY will, in the drafting of and applying to the Regulator for the issue of this Code of Conduct, consult with the Information Regulator, with a view to promoting compliance with PoPIA and a consistency in the approach in this regard.

3. MANDATE AND APPLICATION

- 3.1 By applying to the Information Regulator for the issue of this Code of Conduct the COMPANY confirms that it is acting in terms of the mandate of all of its members at the time that the application is made.
- 3.2 The Company Executive Manager is mandated to, prior to the issue of this Code of Conduct, request the Information Regulator to provide rulings of interpretation on PoPIA that may affect the provisions of this Code of Conduct and to affect non-material amendments to the wording of this Code of Conduct as may be required by the Information Regulator, without further reference to the Company.
- 3.3 This Code of Conduct applies to the Company, in its processing of all information (by definition in PoPIA personal information) in the course of fulfilling its obligations.

4. PURPOSE

4.1 THE PURPOSE OF THIS CODE OF CONDUCT IS TO:

- 4.1.1 Promote appropriate practices by the Company governing the processing of personal information;
- 4.1.2 Encourage the establishment of appropriate agreements between members of the Company and third parties, regulating the processing of personal information as required in PoPIA and dictated by good business practice.
- 4.2 A further purpose of this Code of Conduct is to establish procedures for the COMPANY to be guided in their interpretation of principally PoPIA, but also other law or practices governing the processing of personal information, allowing for complaints against the Company to be considered and remedial action, where appropriate, to be taken.

5. SCOPE

5.1 THIS CODE OF CONDUCT GOVERNS:

- 5.1.1 The processing of personal information by the Company in compliance with PoPIA;
- 5.1.2 Where appropriate, agreements that may need to be concluded between the Company and third parties promoting, and to the extent possible ensuring, that personal information is processed in compliance with PoPIA;
- 5.1.3 The enforcement by the Company of the provisions of this Code of Conduct.

6. DEFINITIONS AND ABBREVIATIONS

6.1 RELEVANT PoPIA DEFINITIONS:

- 6.1.1 **“biometrics”** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
- 6.1.2 **“Child”** Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decisions;
- 6.1.2 **“Code of Conduct”** Means a code of conduct issued in terms of Chapter 7 of PoPIA;
- 6.1.3 **“Competent Person”** Means any person who is legally competent to consent to any action;
- 6.1.4 **“Consent”** Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
- 6.1.5 **“Constitution”** Means the Constitution of the Republic of South Africa, 1996;
- 6.1.6 **“Data Subject”** Means the person to whom personal information relates;
- 6.1.7 **“De-identify”** In relation to personal information of a data subject, means to delete any information that;
- a. Identifies the data subject;
 - b. Can be used or manipulated by a reasonably foreseeable method to identify the data subject;
 - c. Can be linked by a reasonably foreseeable method to other information that identifies the data subject, and “de-identified” has a corresponding meaning;
 - d. “Direct marketing” means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
 - i. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
 - ii. Requesting the data subject to make a donation of any kind for any reason.

- 6.1.8 **“Electronic Communication”** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;
- 6.1.9 **“Enforcement notice”** means a notice issued in terms of section 95;
- 6.1.10 **“Filing System”** means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;
- 6.1.11 **“Information Officer”** of, or in relation to, a:
- a. Public body means an information officer or deputy information officer as
 - b. Contemplated in terms of section 1 or 17; or
 - c. Private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;
- 6.1.12 **“Minister”** means the Cabinet member responsible for the administration of justice;
- 6.1.13 **“Operator”** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;
- 6.1.14 **“person”** means a natural person or a juristic person;
- 6.1.15 **“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.

- 6.1.16 **“Prescribed”** means prescribed by regulation or by a code of conduct;
- 6.1.17 **“Private Body”** means:
- a. A natural person who carries or has carried on any trade, business or profession, but only in such capacity;
 - b. A partnership which carries or has carried on any trade, business or profession; or
 - c. Any former or existing juristic person, but excludes a public body.
- 6.1.18 **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
- a. The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - b. Dissemination by means of transmission, distribution or making available in any other form; or
 - c. Merging, linking, as well as restriction, degradation, erasure or destruction of information.
- 6.1.19 **“Promotion of Access to Information Act”** means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
- 6.1.20 **“Public Body”** means:
- a. Any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government;
 - b. Any other functionary or institution when:
 - i. Exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
 - ii. Exercising a public power or performing a public function in terms of any legislation.
- 6.1.21 **“Public Record”** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

- 6.1.22 **“Record”** means any recorded information:
- a. Regardless of form or medium, including any of the following:
 - i. Writing on 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 any other device in which one or more visual;
 - vi. 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.
- 6.1.23 **“Regulator”** means the Information Regulator established in terms of section 39 of PoPIA;
- 6.1.24 **“Republic”** means the Republic of South Africa;
- 6.1.25 **“re-identify”** in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that –
- (a) Identifies the data subject;
 - (b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
 - (c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject, and **“re-identified”** has a corresponding meaning;
- 6.1.26 **“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;
-

- 6.1.27 **“Restriction”** means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;
- 6.1.28 **“Special Personal Information”** means personal information as referred to in section 26;
- 6.1.29 **“This Act”** includes any regulation or code of conduct made under the Protection of Personal Information Act, 4 of 2013; and
- 6.1.30 **“Unique Identifier”** means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

6.2 RELEVANT COMPANY DEFINITIONS:

- 6.2.1 **“Agreement”** includes an arrangement or understanding between or among two or more parties, which purports to establish a relationship in law between those parties;
- 6.2.2 **“Complainant”** means a person who has filed a complaint in terms of section 136(1);
- 6.2.3 **“Confidential Information”** means personal information that belongs to a person and is not generally available to or known by others;
- 6.2.4 **“Client/Customer/Resident/Employee”**, in respect of an agreement to which this Act applies, means:
- a. The party to whom goods or services are sold to;
 - b. The party who is employed by the Company;
 - c. A person’s education, employment, career, professional or business history, including the circumstances of termination of any employment, career, professional or business relationship, and related matters; or
 - d. A person’s identity, including the person’s name, date of birth, identity number, marital status and family relationships, past and current addresses and other contact details, and related matters;

- 6.2.5 **“Credit”** means when used as a noun, means;
- a. A deferral of payment of money owed to a person, or a promise to defer such a payment; or
 - b. A promise to advance or pay money to or at the direction of another person.
- 6.2.6 **“Juristic Person”** includes a partnership, association or other body of persons, corporate or unincorporated, or a trust if:
- a. There are three or more individual trustees; or
 - b. The trustee is itself a juristic person, but does not include a stokvel.
- 6.2.7 **“Magistrates’ Courts Act”** means the Magistrates’ Courts Act, 32 of 1944;
- 6.2.8 **“Organ of State”** means an organ of state as defined in section 239 of the Constitution;
- 6.2.9 **“Prescribed”** means prescribed by regulation;
- 6.2.10 **“SMS”** means a short message service provided through a telecommunication system;
- 6.3 CODE OF CONDUCT DEFINITIONS:**
- 6.3.1 **“Business Days”** means all weekdays which are not proclaimed public holidays in the Republic of South Africa;
- 6.3.2 **“Company Executive Manager”** means the person appointed by the Company to oversee the conduct of its business.
- 6.4 ABBREVIATIONS:**
- 6.4.1 **“Company”** means a natural legal entity formed by the association which is Willow Acres Estate Homeowners Association
- 6.4.2 **“ISMS”** means an Information Security Management System;
- 6.4.3 **“PAIA”** means the Promotion of Access to Information Act, 2 of 2000;
- 6.4.4 **“PoPIA”** means the Protection of Personal Information Act, 4 of 2013;
- 6.4.5 **“WAHOA”** means the Willow Acres Estate Homeowners Association
-

7. PART B OF THIS CODE OF CONDUCT DEALS WITH EACH OF:

- 7.1 The lawful conditions for Processing of personal information;
- 7.2 The Processing of special personal information; and
- 7.3 The Processing of personal information of children.

8. THE DUTIES AND RESPONSIBILITIES OF THE INFORMATION OFFICER:

- 8.1 Direct marketing by means of unsolicited electronic communications; and
- 8.2 Transfers of personal information outside Republic;
- 8.3 In Parts B and C of this Code of Conduct the relevant provisions of PoPIA are quoted in full, and are identified by being illuminated;
- 8.4 Immediately subsequent to the provisions referred to in 7, reference is made to Other Applicable Legislation relevant to the processing of personal information by the Company.;
- 8.5 Immediately subsequent to the provisions referred to in 7, Other Applicable Legislation, a brief commentary providing guidance to the Company relating to the processing of personal information in compliance with PoPIA in terms of accepted industry practices is provided.
- 8.6 Immediately subsequent to the commentary, the obligations of the Company to comply with PoPIA or actions or omissions that are a functional equivalent in the processing of personal information are stipulated in bold. These provisions do not substitute the stipulations of PoPIA or in any way detract from their operation and must be construed as supplementary to the provisions of PoPIA.

9. COMMENCEMENT OF THE CODE

- 9.1 This Code of Conduct will come into force and be binding on every department/site/branch of the Company at the end of the grace period provided in Section 62(2) of PoPIA, which grace period will commence once the PoPIA commencement date has been affected in the Government Gazette. If no grace period is granted, this Code of Conduct will come into effect and be binding on the COMPANY on the date that PoPIA or any proclamation by the State President requires compliance with those provisions.

- 9.2 Notwithstanding any delays in the commencement of PoPIA or the expiry of transitional arrangements stipulated in Section 114 of PoPIA, the COMPANY encourages its employees to ensure that the processing of personal information complies with PoPIA as early as may reasonably be achieved.

PART B – CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

10. GENERAL

- 10.1 PoPIA takes precedence over any other legislation that regulates the processing of personal information where that legislation is materially inconsistent with an object, or a specific provision of PoPIA, unless the other legislation regulates the processing more extensively than the conditions for lawful processing of personal information, in which event the more extensive provisions will prevail.
- 10.2 Chapter 3 of PoPIA stipulates the conditions for lawful processing of personal information. Codes of Conduct must incorporate these conditions or set out obligations that provide a functional equivalent to the obligations established in the conditions.
- 10.3 In considering the conditions for the lawful processing of personal information the separate conditions must not be considered in isolation. They should be regarded as a constellation of conditions that interact with and may influence the interpretation of the other conditions as circumstances may dictate. For example: The purpose of collecting and processing personal information will impact on whether personal information is adequate, relevant, and not excessive and whether the processing of the personal information is justified. It may also impact on whether the personal information must be collected directly from a data subject and, depending on the scope of the initial purpose, whether further processing is compatible and permissible in terms of PoPIA. The Purpose specification may also influence the period for which personal information may lawfully be retained.
- 10.4 A further example is the requirement for Notification to a data subject were collecting personal information. This is inextricably linked to the provisions in other sections allowing a data subject to access personal information, require the amendment of incorrect personal information and object to the processing of personal information, all of which are dealt with in separate sections of PoPIA dealing with the conditions of lawful processing of personal information.
- 10.5 For the convenience of the reader the full text of each of the conditions for lawful processing of personal information are contained in this Code of Conduct. Definitions applicable to these provisions are also contained in the Definition section of this Code of Conduct.
- 10.6 The Company falls within the definition of “personal information” in PoPIA. In recognition of this PoPIA amends the Company to provide that Sections 68, 70(1), (2)(b) to (g) and (i), (3) and (4) and 72(1), (3) and (5) will be subject to the compliance procedures set out in Chapters 10 and 11 of PoPIA.

- 10.7 It must be noted that while the general principles of processing of personal information stipulated in PoPIA apply to all personal information, the Company shall retain its authority to deal with the filing of consumer/client/employee information.
- 10.8 The provisions governing the processing of information in the Company, while not as extensive as PoPIA, are not inconsistent with PoPIA and the Company complying in this regard will largely comply with the conditions for the lawful processing of personal information contained in PoPIA.
- 10.9 In consequence of their compliance the Company will, in many instances, have developed practices that comply with the conditions for the lawful processing of personal information or practices that constitute functional equivalence of what is required in these conditions. To the extent that it may be appropriate, guidance is provided relating to these practices and the correlation with the conditions for the lawful processing of personal information.
- 10.10 All persons that are subject to this Code of Conduct must comply with the conditions for the lawful processing of personal information stipulated in PoPIA.

11. CONDITION 1: ACCOUNTABILITY

Responsible party to ensure conditions for lawful processing:

- 11.1 The responsible party must ensure that the conditions set out in this section, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.
- 11.2 Other Applicable Legislation:
- 11.2.1 In processing personal information, it is important that the Company establishes in what circumstances they act as responsible parties and in what circumstances they act as operators.
- 11.2.2 By definition a “responsible party” is a person who alone or in conjunction with others, determines the purpose of and means of processing personal information.
- 11.2.3 By definition an “operator” is a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party.
- 11.2.4 In processing personal information, whether as a responsible party or an operator must comply with the conditions for the lawful processing of personal information. The distinction lies in the fact that a responsible party is liable to the data subject and

must ensure that all of the conditions of lawful processing of personal information and measures that give effect to these conditions are complied with. Specifically with regard to Security Safeguards in Condition 7, PoPIA requires that the responsible party must conclude a written contract with the operator and ensure that the operator establishes and maintains the security measures necessary to safeguard the integrity and confidentiality of personal information.

12. CONDITION 2: PROCESSING LIMITATION

Lawfulness of processing:

12.1 PERSONAL INFORMATION MUST BE PROCESSED:

- a. Lawfully; and
- b. In a reasonable manner that does not infringe the privacy of the data subject.

12.2 OTHER APPLICABLE LEGISLATION:

12.2.1 Aside from lawfulness, which would include the sharing of personal information for the purposes of the furtherance of the purposes outside the purpose of the Company, the person processing the information (this is not restricted to the responsible party) must ensure that it is processed in a reasonable manner so as not to infringe the privacy of the data subject;

12.2.2 What is “reasonable”? Reasonableness assumes that all of the conditions of lawful processing is adhered to;

12.2.3 Further, that the data subject has knowledge of:

- a. Who is processing his or her personal information;
- b. The intended use of the personal information; and
- c. Can establish the manner in which the personal information will be handled and secured.

12.2.4 A data subject may reasonably expect that personal information will not be processed where the processing is unjustified or where it may have an unsubstantiated negative effect on the data subject.

12.2.5 If the Company processes personal information in compliance with PoPIA the processing will be lawful, reasonable and will not infringe the privacy of the data subject;

12.2.6 Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

12.3 PERSONAL INFORMATION MAY ONLY BE PROCESSED IF:

12.3.1 The data subject or a competent person where the data subject is a child consents to the processing;

12.3.2 Processing is necessary to carry out actions for the conclusion or performance of a contract;

12.3.3 To which the data subject is party;

12.3.4 Processing complies with an obligation imposed by law on the responsible party;

12.3.5 Processing protects a legitimate interest of the data subject;

12.3.6 Processing is necessary for the proper performance of a public law duty by a public body; or

12.3.7 Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

12.4 The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection 12.3 (1).

12.5 The data subject or competent person may withdraw his, her or its consent, as referred to in subsection 12.3 (1), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection 12.3 (2) to (7) will not be affected.

- 12.6 A data subject may object, at any time, to the processing of personal information:
- a. in terms of subsection 12.3 (d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
 - b. (b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.
- 12.7 If a data subject has objected to the processing of personal information in terms of subsection 12.3, the responsible party may no longer process the personal information.
- 12.8 **“Consent”** means any voluntary, specific and informed expression of will in terms of which permission is given to the processing of personal information.

13. **CONDITION 3: PURPOSE SPECIFICATION**

Section 9 of PoPIA states that personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

The Company collect and process members, their occupants, visitors and employee’s personal information mainly for the purposes of security protocol, financial needs, accuracy, up-to-date, not misleading and complete information for communication purposes. The Company contracts with third parties and thus impose appropriate security, privacy and confidentiality obligations on the third parties to ensure that personal information that we remain responsible is secured. The Company will ensure that anyone to whom the information is passed on to agrees to treat your information with the same level of protection as we are obliged to.

The processing of personal information is only allowed in instances where such personal information is necessary for a Communal Residential Establishment or service provider to conduct business.

The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, the Company will inform the **Client/Customer/Resident/Employee** as to the information required and the information deemed optional. Examples of personal information the company collect include, but is not limited to:

- i. The **Client/Customer/Resident/Employee** Identity Number, name, surname, address, contact number, email address, vehicle details, biometrics, photo picture, citizenship
- ii. Employment history
- iii. Employee banking details for salary payments
- iv. Confirming, verifying and updating **Client/Customer/Resident/Employee** details
- v. Conducting members surveys
- vi. Description of Employees address
- vii. Invoicing purposes
- viii. Any other information required by the Company or its suppliers
- ix. In connection with legal proceedings
- x. In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law
- xi. Providing communication in respect of the Company and regulatory matters that may affect the members

The Company aims to have agreements in place with all Service Providers and Third-Party Service Providers to ensure a mutual understanding with regard to the protection of the **Client/Customer/Resident/Employee** personal information. The Company's Service Providers will be subject to the same regulations as applicable to the Company.

According to Section 10 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the company processing of Personal Information:

- a. The **Client/Customer/Resident/Employee** consents to the processing: - consent is obtained from candidate during the introductory, appointment and needs analysis stage of relationship;
- b. The necessity of processing: in order to conduct an accurate analysis of the **Client/Customer/Resident/Employee** biometric access control, members profiles and contact information for communication
- c. Processing complies with an obligation imposed by law on The Company
- d. Processing protects a legitimate interest of the member – it is in the **Client/Customer/Resident/Employee** best interest to have all relevant personal information to provide them with effective communication and security in order to provide them with an applicable and beneficial product or service.
- e. Processing is necessary for pursuing the legitimate interest of The Company or of a Third Party to whom information is supplied – in order to provide The Company **Client/Customer/Resident/Employee** with products and or services

both The Company and any of our service providers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.

- 13.1 Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;
- 13.2 Steps must be taken in accordance with section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18(4) are applicable.
- 13.3 Other Applicable Legislation:
- a. In Section 68(1) of PoPIA any person who compiles, retains or reports any confidential information must protect the information and only use that information for the purpose permitted or required;
 - b. “Confidential information” is personal information that belongs to a person and is not generally available to or known by others;
 - c. Typically, personal information relating to a person’s financials or name, identity number, phone number, address etc. would be regarded by the data subject as confidential.
- 13.4 If the Company collects information directly from a data subject it must ensure that the data subject is aware of the specific, explicitly defined and lawful purpose related to the function and activity of the Company in processing the data subject’s personal information.
- 13.5 Retention and restriction of records:
- 13.5.1 Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:
 - a. Retention of the record is required or authorised by law;
 - b. The responsible party reasonably requires the record for lawful purposes related to its functions or activities;
 - c. Retention of the record is required by a contract between the parties thereto; or
 - d. The data subject or a competent person where the data subject is a child has consented to the retention of the record.
 - 13.5.2 Records of personal information may be retained for periods in excess of those contemplated in 12.3 for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

- 13.5.3 A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must:
- a. Retain the record for such period as may be required or prescribed by law or a code of conduct; or
 - b. If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.
- 13.5.4 A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record.
- 13.5.5 The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.
- 13.5.6 The responsible party must restrict processing of personal information if:
- a. its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;
 - b. the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;
 - c. the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
 - d. the data subject requests to transmit the personal data into another automated processing system.
- 13.5.7 Personal information referred to may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.
- 13.5.8 Where processing of personal information is restricted pursuant to subsection 13.5.6, the responsible party must inform the data subject before lifting the restriction on processing.

14. CONDITION 4: FURTHER PROCESSING LIMITATION

- 14.1 Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of Section 13 of the PoPIA;
- 14.2 To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of:
- a. The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
 - b. The nature of the information concerned;
 - c. The consequences of the intended further processing for the data subject;
 - d. The manner in which the information has been collected; and
 - e. Any contractual rights and obligations between the parties.
- 14.3 The further processing of personal information is not incompatible with the purpose of collection if:
- 14.3.1 The data subject or a competent person where the data subject is a child has consented to the further processing of the information;
- 14.3.2 The information is available in or derived from a public record or has deliberately been made public by the data subject;
- 14.3.3 Further processing is necessary:
- 14.4 To avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
- 14.5 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
- 14.6 For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
- 14.7 In the interests of national security;
- 14.8 The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:
- i. public health or public safety; or
 - ii. the life or health of the data subject or another individual;

- 14.9 The information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
- 14.10 The further processing of the information is in accordance with an exemption granted under section 37 of the PoPIA.

15. CONDITION 5: INFORMATION QUALITY

- 15.1 A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.
- 15.2 In taking the steps referred to in subsection 14.1, the responsible party must have regard to the purpose for which personal information is collected or further processed.

16. CONDITION 6: OPENNESS

- 16.1 A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

Note: Section 14 of the Promotion of Access to Information Act applies to public bodies and as the Company is by definition a private body in terms of that Act, Section 14 is not applicable and only section 51 is applicable.

16.2 OTHER APPLICABLE LEGISLATION:

The Promotion of Access to Information Act, 2 of 2000:

In Section 51 provides:

- 16.2.1 **Within six months after the commencement of this section or the coming into existence of the private body concerned the head of a private body must compile a manual containing:**
- a. The postal and street address, phone and fax number and, if available, electronic mail address of the head of the body;
 - b. A description of the guide referred to in section 10, if available, and how to obtain access to it;

- c. The latest notice in terms of section 52 (2), if any, regarding the categories of record of the body which are available without a person having to request access in terms of this act;
 - d. A description of the records of the body which are available in accordance with any other legislation;
 - e. Sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject; and
 - f. Such other information as may be prescribed.
- 16.2.2 The head of a private body must on a regular basis update the manual referred to in Subsection (1).
- 16.2.3 Each manual must be made available as prescribed.
- 16.2.4 For security, administrative or financial reasons, the Minister may, on request or of his or her own accord, by notice in the Gazette, exempt any private body or category of private bodies from any provision of this section for such period as the Minister thinks fit.”
- 16.3 A fundamental purpose of PoPIA is to allow the data subject access to and knowledge of his or her personal information that is being processed by either of, or both responsible parties and operators. Even if the data subject has knowledge through collection of the information directly from him or her or notification as required in Section 18 of PoPIA, if the information indicating how the personal information is being processed is not available to the data subject, he or she may be prevented from exercising the right to require amendment of inaccurate personal information or object to the processing of personal information, as stipulated in PoPIA.
- 16.4 If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of.
- 16.5 The steps referred to in 16.3 must be taken:
- a. if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or
 - b. in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.
- 16.6 A responsible party that has previously taken the steps referred to in subsection 15.7 complies in relation to the subsequent collection from the data subject of the same

information or information of the same kind if the purpose of collection of the information remains the same.

- 16.7 It is not necessary for a responsible party to comply with subsection 16.3 if:
- a. The data subject or a competent person where the data subject is a child has provided consent for the non-compliance;
 - b. Non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this act;
 - c. Non-compliance is necessary:
 - i. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
 - ii. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
 - iii. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
 - iv. in the interests of national security;
 - d. Compliance would prejudice a lawful purpose of the collection;
 - e. Compliance is not reasonably practicable in the circumstances of the particular case; or
 - f. The information will:
 - i. not be used in a form in which the data subject may be identified; or
 - ii. be used for historical, statistical or research purposes.
- 16.8 To enable data subjects to exercise their rights relating to the processing of their information a critical prerequisite is knowledge of the who, how and what relating to their personal information. Without this knowledge the data subject is deprived of the right to object to the processing of their personal information, prevent direct marketing, establish where automated decision-making may adversely affect them, and correct inaccurate personal information.

17. CONDITION 7: SECURITY SAFEGUARDS

It is a requirement of POPI to adequately protect personal information. The Company will continuously review its security controls and processes to ensure that personal information is secure.



- 17.1 A responsible party 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:
- 17.1.1 Loss of, damage to or unauthorised destruction of personal information; and

- 17.1.2 Unlawful access to or processing of personal information.
- 17.2 In order to give effect to section 17.1, the responsible party must take reasonable measures to:
 - 17.2.1 Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
 - 17.2.2 Establish and maintain appropriate safeguards against the risks identified;
 - 17.2.3 Regularly verify that the safeguards are effectively implemented; and
 - 17.2.4 Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- 17.3 The responsible party must 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.
- 17.4 The following procedures are in place in order to protect personal information:
 - 17.4.1 The Company Information Officer is the Chairperson whose details are available in this document and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. The Chairperson is assisted by the Estate Manager who will function as the Company's Information Officer.
 - 17.4.2 This Code of Conduct has been put in place throughout the Company and training on this policy and the POPI Act has already taken place and will be conducted by the Company
 - 17.4.3 Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI
 - 17.4.4 Every employee currently employed within The Company will be required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
 - 17.4.5 The Company archived **Client/Customer/Resident/Employee** information is stored on site which is also governed by POPI, access is limited to these areas to authorised personal.
 - 17.4.6 The Company suppliers, services provers, insurers and other third-party service providers will be required to sign a Service Level Agreement or an addendum to their agreements guaranteeing their commitment to the Protection of Personal Information, this is however a ongoing process that will be evaluated as needed.
 - 17.4.7 All electronic files or data on employees' laptops are Backed Up by BHudson T/A Hudson IT Solution which is also responsible for system security that protects third party access and physical threats.


- 17.4.8 All hard copy of members properties and personal information are stored in a lockable filing cabinet and or behind a secured lock gate. Only authorised personal can have access to these documents.
- 17.4.9 All data collected for storing of **Client/Customer/Resident/ Visitors** via our Visitor Management System as well as Customer Management System are managed by the appointed Services Provider Glovent Solutions which is also responsible for system security that protects third party access and physical threats. The Glovent Groups is responsible for Electronic Information Security. They have implemented Technical Measures to protect Client Data on a high level, the following technical measures are in place to protect the client data:
- a) GLOvent currently monitors security recommendation's, standards and best practices from organizations such as OWASP (www.owasp.org) and others to ensure our products and services are as secure as possible. It must be noted that no system can ever be "tamper" or "hack proof", this has been proven by the many successful attacks against some of the biggest online services in the world. GLOvent takes appropriate measures to prevent and minimize risks of unauthorized access to, improper use and the inaccuracy of the customer's personal information.
 - b) GLOvent will not disclose any personal information to a person/company who is not directly involved in the delivery of their products/services or without the customer's permission, unless compelled by law/in terms of a court order to do so, or in public interest or necessary to protect the rights and ensure the integrity and operation of its business and systems.
 - c) GLOvent uses enterprise standard technology such as MYSQL RDMS, Java Programming Language and Jboss Application Server. These technologies are tried and tested and used by a vast array of businesses around the world to create secure systems.
 - d) GLOvent adheres to industry practices in terms of securing the servers that the GLOvent products are hosted upon, these practices include, but are not limited to, the use of Anti-Virus, RootKit Checking software, Secure Firewall Software and other best practice configuration standards.
 - e) SSL (Secure Sockets Layer) is used by GLOvent to establish an encrypted link between our servers and a web browser accessing the the GLOvent products. SSL is a connection standard security technology. (see details of our SSL Security Certificate at the end of this document).
 - f) The GLOvent Systems and Data are hosted Amazon Web Services (AWS) located in Ireland.

Commercial Measures Implemented to protect Client Data:

- i. Data security (with specific reference to the member’s personal information) is detailed in our standard Service Agreement. It is stated that GLOVent is not allowed to use the database for any other purpose than for the fulfilment of their agreement and is not allowed to make know or disseminate the database or any part thereof to any third party that is not directly involved in the delivery of the contracted products and/or services.
- ii. The Service Agreement also specifically notes that all data (including the member database, design elements, etc.) remains the property of the client and that GLOVent is to return this data to the client, and destroy any copies thereof, if requested.
- iii. Details of GLOPortal SSL Security Certificate:
COMODO SSL Analyzer v1.0.13 Report for: cms.gloportal.co.za:
Certificate Details

Common Name	ssl381754.cloudflaressl.com	
Subject Name	commonName=ssl381754.cloudflaressl.com organizationalUnitName=PositiveSSL Multi-Domain organizationalUnitName=Domain Control Validated	
Serial Number	<u>4C7A5BD795E29CCDA0B8D013D07AC91C</u>	
Fingerprint (SHA-256)	<u>98BAB292B8BE48D5B13317727393D9758FCC6AE726CE07D0E1D2CC83A42445CE</u>	
Valid From	Thu, 27 Apr 2017 00:00:00 GMT	
Valid To	Fri, 03 Nov 2017 23:59:59 GMT	
Key	EC (256-bit)	
Signature	SHA-256 / ECDSA	
Issuer Name	commonName=COMODO ECC Domain Validation Secure Server CA 2 organizationName=COMODO CA Limited localityName=Salford stateOrProvinceName=Greater Manchester countryName=GB 	
Issuer Brand	COMODO	 Creating Trust Online®
Validation Type	Domain Validated (DV)	
Trusted by Microsoft?	Yes	
Trusted by Mozilla?	Yes	

<i>Certificate Status Details</i>	
OCSP "Stapling"	Good This Update: Sun, 09 Jul 2017 20:24:39 GMT Next Update: Sun, 16 Jul 2017 20:24:39 GMT
Must Staple? (TLS Feature)	No
<i>Server Details</i>	
Software	cloudflare-nginx
IP Address	104.24.24.61
Port	443
Hostname	Unknown
Clock (ServerHello.gmt_unix_time)	Thu, 13 Jul 2017 08:49:44 GMT (Accurate)
Clock (HTTP "Date:" header)	Thu, 13 Jul 2017 08:49:44 GMT (Accurate)
<i>Protocol Versions</i>	
TLS v1.2	Supported Immune to TLS POODLE attack i
TLS v1.1	Supported Immune to TLS POODLE attack i
TLS v1.0	Supported Immune to TLS POODLE attack i
SSL v3.0	Not Supported Immune to SSLv3 POODLE attack i
SSL v2.0	Not Supported Immune to DROWN attack i
<i>Protocol Features / Problems</i>	
Downgrade Protection (TLS_FALLBACK_SCSV)	Supported
Secure Renegotiation (Server-initiated)	Supported
Secure Renegotiation (Client-initiated)	Not Supported
Legacy Renegotiation (Client-initiated)	Not Supported
Compression	Not Supported Immune to CRIME attack i
Heartbeat	Not Supported Immune to Heartbleed attack i
Server Name Indication	Supported
Session Resumption	Supported
Session Tickets	Supported
TLS Extension Intolerant?	No
Cipher Suite Negotiation Bug?	No

Signature Algorithms Enabled	None Immune to SLOTH attack 
<i>Cipher Suites Enabled</i>	
Name (ID)	Key Size (in bits)
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC14)	256 ECDH 256-bit (P-256)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC02B)	128 ECDH 256-bit (P-256)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)	128 ECDH 256-bit (P-256)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)	128 ECDH 256-bit (P-256)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC02C)	256 ECDH 256-bit (P-256)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)	256 ECDH 256-bit (P-256)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)	256 ECDH 256-bit (P-256)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC13)	256 ECDH 256-bit (P-256)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)	128 ECDH 256-bit (P-256)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)	128 ECDH 256-bit (P-256)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)	128 ECDH 256-bit (P-256)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9C)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2F)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3C)	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)	256 ECDH 256-bit (P-256)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)	256 ECDH 256-bit (P-256)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)	256 ECDH 256-bit (P-256)
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9D)	256

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3D)	256
<i>Miscellaneous</i>	
Report Date	Thu, 13 Jul 2017 08:49:44 GMT
Report Duration	1 second

© COMODO CA Limited 2010-2016. All rights reserved.

SECURITY IMPLEMENTATION CHECKLIST			
Premises	Date	Comment	Recommended Intervention
Inspection of physical security & access			
Access control, cards, tags and biometrics			
Burglar Bars			
Alarm & deactivation codes			
Armed Response			
No-go areas, demarcated			
Risk analysis of security issues			
Filing and Physical Record Keeping			
Locked offices and Cabinets			
No-go areas			
Proper disposal of records/files/hard copy – shredding policy			
Work/document flow – data remains secure			
File integrity & lockup			
Staff			
Keys to authorised employees only			
Alarm codes			
Area Specific Access			
Staff are aware of their POPI obligations			
Third Party Processing			
External Operators all have written contracts			
External Operators are aware of data usage security and limitations			
External Operators Confidentiality requirements			
Inspection of 3 rd Parties premises, systems and compliance			
IT and Data			
Computers physical secured			
Password Policy			
Encryption of data			
Back-ups policy and schedule			
Person appointed to manage backups			
Off-site storage			
Proper disposal of damaged devices/data drives			
Network, Internet and www.security			
Mobile Devices			
No flash drives / removable media in restricted areas			
Private devices not permitted to sync on networks			
Laptop – data encrypted			
Laptop – password secured			
Theft prevention strategy			
Security Breaches			
Any loss of data/security breach the regulator			
Any loss of data / security breach the data subjects			

18. CONDITION 8: DATA SUBJECT PARTICIPATION

- 18.1 A data subject, having provided adequate proof of identity, has the right to:
- 18.1.1 Request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and
 - 18.1.2 Request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:
 - a. within a reasonable time;
 - b. at a prescribed fee, if any;
 - c. in a reasonable manner and format; and
 - d. in a form that is generally understandable.
 - 18.1.3 If, in response to a request, personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.
 - 18.1.4 If a data subject is required by a responsible party to pay a fee for services provided to the data subject to enable the responsible party to respond to a request, the responsible party:
 - a. must give the applicant a written estimate of the fee before providing the services; and
 - b. may require the applicant to pay a deposit for all or part of the fee.
- 18.2 A responsible party may or must refuse, as the case may be, to disclose any information requested to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply.
- 18.3 The provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records.
- 18.4 If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection 18.2, every other part must be disclosed.

Note: *The Company is prohibited from processing health records and therefore the provisions of Section 61 of the Promotion of Access to Information Act is not applicable.*

- 18.5 Correction of personal information. A data subject may, in the prescribed manner, request a responsible party to:
- a. Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
 - b. Destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of Section 14.
- 18.6 On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable:
- a. correct the information;
 - b. destroy or delete the information;
 - c. provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or
 - d. where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
- 18.7 If the responsible party has taken steps that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.
- 18.8 The responsible party must notify a data subject, who has made a request of the action taken as a result of the request.
- 18.9 Manner of access. The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of section 23 of this Act.

19. PROCESSING OF SPECIAL PERSONAL INFORMATION

19.1 Prohibition on processing of special personal information:

19.1.1 A responsible party may, subject to section 27, not process personal information concerning:

- a. 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
- b. the criminal behaviour of a data subject to the extent that such information relates to:
 - i. the alleged commission by a data subject of any offence; or
 - ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

19.2 The Company is expressly prohibited from processing information that correlates closely to the provisions of Section 26(a) of PoPIA.

19.3 Section 26 further prohibits the processing of personal information relating to criminal behaviour, in respect of which a data subject has not yet been found guilty of an offence. This is not directly addressed in the Company Regulations, but the Company does not process information of this nature.

20. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

20.1 A responsible party may not process personal information concerning a child.

20.2 General authorisation concerning personal information of children:

20.2.1 The prohibition on processing personal information of children, as referred to in section 34, does not apply if the processing is:

- a. Carried out with the prior consent of a competent person;
- b. Necessary for the establishment, exercise or defence of a right or obligation in law;
- c. Necessary to comply with an obligation of international public law;
- d. For historical, statistical or research purposes to the extent that:
 - i. the purpose serves a public interest and the processing is necessary for the purpose concerned; or
 - ii. 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 child to a disproportionate extent; or
- e. Of personal information which has deliberately been made public by the child with the consent of a competent person.

- 20.2.2 The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.
- 20.2.3 The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must:
- a. Upon request of a competent person provide a reasonable means for that person to:
 - i. review the personal information processed; and
 - ii. refuse to permit its further processing;
 - b. Provide notice:
 - i. regarding the nature of the personal information of children that is processed;
 - ii. how such information is processed; and
 - iii. regarding any further processing practices;
 - c. Refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and Establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

21. DISCLOSURE OF PERSONAL INFORMATION

The Company may disclose a client's personal information of any of the Company's third-party services providers whose service products **Client/ Customer/ Resident/ Employee** appoint to use. The Company has agreements in place to ensure that compliance with confidentiality and privacy conditions.

The Company may also share **Client/Customer/Resident/Employee** personal information with, and obtain information about **Client/Customer/Resident/Employee** from third parties for the reasons already discussed above.

The Company may also disclose a candidate's information where it has a duty or right to disclose in terms of applicable legislations, the law, or where it may be deemed necessary in order to protect The Company rights.

22. ACCESS AND CORRECTION OF PERSONAL INFORMATION

Client/Customer/Resident/Employee have the right to access the personal information the Company holds about them. **Client/Customer/Resident/Employee** also have the right to ask the Company to update, correct or delete their personal information on reasonable grounds. Once a **Client/Customer/Resident/Employee** objects to the processing of their personal information, the Company may no longer process said personal information. The Company will take all reasonable steps to confirm **Client/Customer/Resident/Employee** identity before providing details of their personal information or making changes to their personal information. FORM 2 Annexed hereto can be completed to correct / delete / destroy personal information.

23. AMENDMENTS TO THIS CODE OF CONDUCT

Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year. **Client/Customer/Resident/Employee** are advised to access the Clients website periodically to keep abreast of any changes. Where material changes take place, **Client/Customer/Resident/Employee** will be notified directly or changes will be stipulated on the Client's website.

24. NOTIFICATION OF SECURITY COMPROMISES

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify:

- 24.1. The Regulator; and
- 24.2. The data subject, unless the identity of such data subject cannot be established.
- 24.3. The notification referred to must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.
- 24.4. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

- 24.5. The notification to a data subject referred to must be in writing and communicated to the data subject in at least one of the following ways:
- 24.5.1. Mailed to the data subject's last known physical or postal address;
 - 24.5.2. Sent by e-mail to the data subject's last known e-mail address;
 - 24.5.3. Placed in a prominent position on the website of the responsible party;
 - 24.5.4. Published in the news media; or
 - 24.5.5. As may be directed by the Regulator.
- 24.6. The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:
- 24.6.1. Description of the possible consequences of the security compromise;
 - 24.6.2. A description of the measures that the responsible party intends to take or has taken to address the security compromise;
 - 24.6.3. A recommendation with regard to the measures to be taken by the data subject to mitigate;
 - 24.6.4. The possible adverse effects of the security compromise;
 - 24.6.5. If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.
 - 24.6.6. The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

25. OTHER APPLICABLE LEGISLATION:

It is accepted globally that data subjects have the right to know if the security of their personal information has been compromised. It is the data subject who is best placed to protect him or herself against the abuse of their personal information but unless the data subject has knowledge of the compromise they are deprived of this right.

Financial information is by its nature valuable and is typically regarded as sensitive. This is illustrated by the fact that in Chapter 11 of PoPIA dealing with Offences, Penalties and Administrative Fines unlawful acts by responsible parties and third parties in connection with "account numbers" receive special attention.

THE COMPANY MUST:

Establish appropriate mechanisms to immediately notify the Regulator when reasonable grounds exist to believe that personal information of a data subject has been compromised;

PART C – ACTS, POLICIES AND PROCEDURES

26. THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

PURPOSE

To exercise effective control over the retention of documents and electronic transactions:

- a. as prescribed by legislation; and
- b. as dictated by business practices

Documents need to be retained in order to prove the existence of facts and to exercise rights the Company may have. Documents are also necessary for defending legal action, for establishing what was said or done in relations to business of the Company and to minimize the Company's reputational risks.

To ensure that the Company's interests are protected and that the Company's right to privacy and confidentiality is not breached. Queries may be referred to the Information Officer

SCOPE AND DEFINITIONS

All documents and electronic transactions generated within and/or received by the Company.

- a. Definitions
 - i. Client/Customer/Resident/Employee includes, but are not limited to, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.
 - ii. Confidential Information refers to all information or data disclosed to or obtained by the Company by any means whatsoever.
 - iii. Constitution: Constitution of the Republic of South Africa Act, 108 of 1996
 - iv. Data refers to electronic representations of information in any form
 - v. Documents include books, records, accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form
 - vi. ECTA: Electronic Communications and Transactions Act, 25 of 2002
 - vii. Electronic communication refers to a communication by means of data message
 - viii. Electronic signature refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.
 - ix. Electronic transactions include emails sent and received
 - x. PAIA: Promotion of Access to Information Act, 2 of 2002

27. ACCESS TO DOCUMENTS

All company and **Client/Customer/Resident/Employee** information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause below):

- Where disclosure is under compulsion of law
- Where there is a duty to the public to disclose
- Where the interests of the Company require disclosure, and
- Where disclosure is made with the express or implied consent of the client

28. DISCLOSURE TO 3RD PARTIES

All employees have a duty of confidentiality in relation to the Company/ **Client/Customer/ Resident/ Employee**

- Information on clients and candidates: Our **Client/Customer/Resident/Employee** right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd Party if the **Client/Customer/Resident/Employee** has consented in writing to that person receiving the information.
 - Request for company information:
 - These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company must however refuse access to records if disclosure would constitute and action for breach of the duty of secrecy owed to a third party.
 - In terms hereof, requests must be made in writing on the prescribed form to the Company Secretary, who is also the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.
 - Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be kept strictly confidential at all times.
- The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

29. STORAGE OF DOCUMENTS

29.1 Hard Copies

Documents are stored in lockable storage at the Company's Offices.

29.2 Electronic Video Recordings / Security Video footages

29.2.1 The Data Protection Act requires organisations to protect any "personal data" that they hold relating to individuals. Personal data is not just restricted to written text; CCTV recordings also fall within the scope if individuals can be identified from them.

29.2.2 The Company installs and operates closed-circuit television ("CCTV") surveillance infrastructure in Residential Estate. The real-time surveillance services are approved to provide security services on behalf of residents' association.

29.2.3 The cameras are positioned so that they record public streets, communal areas, Estate Offices and Clubhouse, Playground and recreational facility and pedestrian walkways. Footage of these areas is recorded and stored for a limited amount of time.

29.2.4 The Company undertakes to ensure that its employees, directors, affiliates, partners and/or clients adhere to the strictest levels of confidentiality and respect individual's right of privacy.

ACCOUNTABILITY

29.2.5 The Company "processes" "Personal Information" (which contained in the CCTV surveillance footage) as contemplated in the Protection of Personal Information Act, No. 4 of 2013 (the "Act"), at all times taking into account individual's constitutional right to privacy.

29.2.6 The authorisation for the collection, location and access of the CCTV surveillance footage ("Data") lies with the Company. The Data may then be accessed, through The Company's systems, with the Company's express prior written consent.

29.2.7 To the extent that the Company gathers the Data, contracted to Elf Rentals, Elf Rentals is acting in the capacity of an "Operator" as defined in the Act. To the extent that the company can be considered to be the party responsible for

"processing" the Data. The Company is acting in the capacity of a "Responsible Party", as defined in the Act.

- 29.2.8 The Company shall fully comply with its obligations in terms of the Act, depending on the capacity in which it is acting any given circumstance.
- 29.2.9 The Company will be processing Personal Information where, given the purpose for which it is processed, such processing is adequate, relevant and not excessive.
- 29.2.10 Details and records of all information processed by the Company will be maintained to the extent required by law.

PURPOSE

- 29.2.11 The purpose of this policy is to outline the Company's approach to the use of CCTV surveillance for purposes in line with the Act. Specifically, the Company strives to:
- 29.2.11.1 process any Data lawfully, and in reasonable manner which does not unreasonably infringe on the privacy of the data subject;
 - 29.2.11.2 only process Data where, to do so, protects a legitimate interest of members of the public;
 - 29.2.11.3 ensure each individual's constitutional right to privacy, by safeguarding Personal Information when processed by it or any of its customers (each of which constitutes a Responsible Party in terms of the Act), subject to justifiable limitations;
 - 29.2.11.4 balance the privacy rights of individuals against other rights, particularly the rights of members of the general public to safety and security;
 - 29.2.11.5 regulate the manner in which Data may be processed, by establishing conditions in accordance with locally applicable laws and international standards, that prescribe the minimum threshold requirements for the lawful processing of Personal Information;
 - 29.2.11.6 advise individuals of their rights and remedies in order to protect their Personal Information from processing that is not in accordance with the Act; and
 - 29.2.11.7 comply with voluntary and compulsory measures, including those established by the Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by the Act.
 - 29.2.11.8 The purpose of the Company's CCTV surveillance network is to:

- 29.2.11.8.1 detect, deter and prevent crime;
 - 29.2.11.8.2 enhance safety of those who live, work and visit the areas covered by the CCTV surveillance network;
 - 29.2.11.8.3 assist in the apprehension and prosecution of offenders (including but not limited to the use of images and video as evidence in criminal/civil proceedings);
 - 29.2.11.8.4 assist law enforcement agencies, including private armed response and security companies, with regard to the investigation of any apparent or actual crime that may be captured by the CCTV surveillance network;
 - 29.2.11.8.5 identify vehicles which may have been involved in criminal activities in order to alert the relevant authorities;
 - 29.2.11.8.6 assist in the maintenance of public order and the reduction of vandalism, theft and related property crimes; and
 - 29.2.11.8.7 promote the safety, protection and wellbeing of members of the public generally.
- 29.2.11.9 Data gathered by the CCTV surveillance network will not be used for any purposes other than those listed above and/or permitted by the Act.
- 29.2.11.10 Data will not, under any circumstances, be released to the media or any similar outlet, nor will any Data be released or disseminated unless specifically required or authorised by law.

SCOPE AND OPERATION

- 29.2.11.11 The Company's CCTV surveillance network employs fixed cameras, designed and deployed to record images of individuals, as well as vehicle and vehicle registration plates, on public roads and in public spaces.
- 29.2.11.12 The CCTV surveillance network will be operated, and Data will only be made available, consistent with the requirements and restrictions imposed by the Act, always taking into account each individual's right to privacy.
- 29.2.11.13 All Data recorded on the CCTV network shall be reviewed by the operational staff, who will monitor the CCTV surveillance feed for

- the purpose of assisting with the identification and prevention of criminal activity and in the interests of public safety and security.
- 29.2.11.14 Software, which works in combination with the Data captured by the CCTV surveillance network, is able to identify registration plates affixed to vehicles. Recorded registration plates are run through a database of registration plates for vehicles which have been involved in a crime or are of interest to the South African Police Services and, should there be any matches, the company monitoring the CCTV camera will be notified. The Company does not have the ability to query registration plate details against the national eNatis database and accordingly any information regarding ownership of a particular vehicle (e.g. identity number, name, physical address) is not accessible unless this information was included when a vehicle was reported as stolen.
- 29.2.11.15 The Company and/or its duly contracted companies and/or the South African Police Services will be directed to respond, where possible, to information provided by companies utilising Data supplied by the Company. The Company does not monitor the Data, nor will it actively perform and crime prevention activities. These activities will be carried out by the appropriate security companies or the South African Police Services.
- 29.2.11.16 Any company appointed by the company will be required to act within the law and will not be authorised to carry out the duties of the South African Police Services.
- 29.2.11.17 All Data will be stored on hosted servers and identified using an automatic recording sequence. The Data will be stored for a period of at least 8 days, being the length of time, the Data is required to be maintained in order to achieve the purpose for which it was collected.
- 29.2.11.18 This retention period may be increased or decreased in line with any lawful instruction provided by the Information Regulator or other competent authority from time to time. Data may be stored for a longer period should it be required for further investigation.
- 29.2.11.19 At the expiry of this retention period, the data will be permanently deleted and/or destroyed in accordance with POPIA stipulated guidelines.
- 29.2.11.20 The fixed CCTV surveillance network will be installed in strategic areas and will be installed in such a manner that all CCTV surveillance cameras are and will be clearly visible and identifiable to members of the public. The CCTV surveillance cameras will be situated in, and will cover, only areas in which the public has

unrestricted access and areas that are within public view. In certain circumstances, a natural or juristic person may request private surveillance solutions in which case CCTV surveillance cameras may be deployed such that private spaces belonging to that person are under surveillance.

- 29.2.11.21 No cameras will be hidden or obscured, nor will they be placed in such a fashion that any camera will be able to record activity in any area which is not considered to be 'public' (for example, into private driveways or over private boundary walls).
- 29.2.11.22 All captions inserted onto collected Data, such as camera location, time and date, are securely maintained and stored and are incapable of being tampered with.

PUBLIC AWARENESS OF CCTV SURVEILLANCE

- 29.2.11.23 Prior to the deployment of CCTV cameras, the company, together with any interested security providers and/or residents' associations, will use all reasonable efforts to advise those residing and/or travelling in the area of its intention to CCTV surveillance in that area.
- 29.2.11.24 In order to ensure that all members of the public entering any area in which the CCTV surveillance network operates are informed of the surveillance, prominent signs will be posted in these areas.
- 29.2.11.25 The signs will direct any interested person to information relating to the Data recorded, contact details of the company or companies monitoring the specific camera, details regarding access to the Data and all relevant contact details, and each person's rights in terms of the Act.

RETENTION OF DATA AND SECURITY OF DATA

- 29.2.11.26 Data will be retained for up to 8 days, unless it is required and requested for purposes outlined in this policy which would require that the data be stored for a longer period. Appropriate safeguards will be put in place should such Data be retained for longer periods, as required by the Act.
- 29.2.11.27 Data retained for purposes of investigation will be strictly managed with limited access. Any Data requested by the South African Police Services will only be released upon presentation of the appropriate subpoena.

- 29.2.11.28 All Data will be stored on secure servers leased or owned by the company. The company will ensure that all Data is stored in a secure server environment that uses modern, advanced security systems to prevent loss of, damage to or unauthorised destruction of Data, and unauthorised access to or processing of Data.
- 29.2.11.29 Members will not be entitled to download and store Data without having submitted a specific, written request to the company. The request will be required to set out the reason and purpose of the download and the duration for which the Data will be stored, along with strict security undertakings, which request the company will refuse if it is not satisfied with the reasons provided or that the Data will be securely stored.
- 29.2.11.30 After a period of 30 days (or such longer period as may be required per the above), the Data will be permanently erased and/or destroyed.

ACCESS TO CCTV SURVEILLANCE DATA BY CONTRACTED COMPANIES

- 29.2.11.31 Only specific persons within the company will have the ability to access and review Data recorded by the CCTV surveillance network, and then only on a "need to know" basis.
- 29.2.11.32 These individuals include, from time to time:
- 29.2.11.32.1 the Directors of the Company;
 - 29.2.11.32.2 the Information Officer of the Company;
 - 29.2.11.32.3 employees who are required to support or maintain the system;
 - 29.2.11.32.4 specified employees or company appointed by the company to monitor and/or retrieve Data; all of whom shall conclude the necessary confidentiality and security undertakings in terms of which each individual with access to any Data will undertake to access such Data only as and when required to do so.
- 29.2.11.33 They shall not be entitled to share or distribute any Data unless required in order to give effect to the purpose for which the Data is recorded, or as required by law.
- 29.2.11.34 Any security company contracted to the Company in order to monitor the Data will, at all times, be registered with the Private Security Industry Regulatory Authority.

- 29.2.11.35 The Information Officer, or other designated officer, will have the following responsibilities:
- 29.2.11.35.1 conduct an annual review of CCTV surveillance network and usage;
 - 29.2.11.35.2 ensure that CCTV images are being stored securely and handled in accordance with this policy, the Act and all applicable laws;
 - 29.2.11.35.3 ensure that images are properly retained and stored, and that all electronic records are managed as any sensitive personal record would be within the organisation;
 - 29.2.11.35.4 ensure that Data is disposed of in the manner required by the Act;
 - 29.2.11.35.5 ensure that any Data which is stored on any external storage system is securely encrypted;
 - 29.2.11.35.6 ensure access protocols are in place and are being followed by all personnel with access to any Data;
 - 29.2.11.35.7 ensure that viewing and disclosure of images is in line with the company policy and legal obligations;
 - 29.2.11.35.8 ensure that staff using or maintaining the CCTV systems are sufficiently trained and aware of their obligations under the Act and any other applicable laws;
 - 29.2.11.35.9 ensure that each system is regularly maintained and identify if system upgrades are necessary; and
 - 29.2.11.35.10 ensure that each passive CCTV system has adequate signage advising members of the public and staff that they are being monitored.
- 29.2.11.36 Employees of any company which contracts with the company to monitor and review any Data in order to give effect to the purpose for which the Data is collected, will be subject to security background checks. All such employees will be required, as condition of their employment, to submit to various confidentiality undertakings relating to access to, and use of, the Data, will only be able to view the Data in controlled monitoring environments and will be subject to constant oversight and supervision.
- 29.2.11.37 Any unlawful disclosure of any Data, or any breach of any provision of the Act or any contract, shall be immediately addressed and, to the extent necessary, the breach will be

reported to the Information Regulator, together with all details relating to the breach, as required in terms of the Act.

ACCESS TO DATA BY PRIVATE INDIVIDUALS

- 29.2.11.38 Individuals have the right to access Data of themselves in terms of the Act. Individuals may request that the relevant responsible party confirm, free of charge, whether the individual has been recorded on the CCTV network.
- 29.2.11.39 Individuals who have concerns over a potential infringement of their privacy may request a review of camera operations by contacting the parties responsible for monitoring the Data.
- 29.2.11.40 The requests for access to Data must include:
- 29.2.11.40.1 exact date and time the images were recorded;
 - 29.2.11.40.2 information to identify the individual (if necessary);
 - 29.2.11.40.3 proof of identity; and
 - 29.2.11.40.4 location/area of the CCTV camera presumed to have recorded the Data.
 - 29.2.11.40.5 The party responsible for monitoring the Data in question shall promptly respond to the request.
- 29.2.11.41 In accordance with the Act, the party responsible for monitoring the Data in question may provide a record or a description of the Data that it has in its possession. A downloadable copy of the Data shall only be provided if, in the opinion of the responsible party, the Data requested does not contain personal information of anyone other than the requesting party and/or will be maintained safe and secure.
- 29.2.11.42 A reasonable fee will be charged for access to the Data, which fee shall be determined with reference to the time, technical expertise and resources which are required to expended on retrieving the Data and, where necessary, sanitising and de-identifying the Data to ensure no third-party rights are affected. The requesting party will be provided with a quotation for this fee as required by the Act.
- 29.2.11.43 If the Company cannot comply with the request, reasons shall be documented. The individual shall be advised of the reasons in writing, where possible.
- 29.2.11.44 Data will only be disclosed to third parties (being parties other than those acting on behalf of contracted companies or private individuals on their own behalf) if subpoenaed to do so, or otherwise compelled by law.

- 29.2.11.45 Access to the Data will only be released to third parties in terms of the Act or in terms of the Promotion of Access to Information Act (“PAIA”). Whichever may be applicable.

29.3 Minimum period of retention

- 29.3.1 The periods of retention specified in the Code in respect of each statute listed, are minimum periods of retention and they are applicable to both electronic and non-electronic records. Records can be retained for longer periods provided there is no legislation that imposes a maximum period of retention.
- 29.3.2 If different retention periods are stipulated in different pieces of legislation in respect of the same record, the record must be retained for the longer period.
- 29.3.3 If legislation requires that a record be kept indefinitely, this obligation is satisfied if the record is kept for the period of existence of the person that is subject to the retention obligation. In certain instances, such as the deregistration or insolvency of a company, it is advisable to retain records after it has ceased to exist if there is a potential for litigation or if there is a possibility that the company may be re-registered.
- 29.3.4 Records which a company is required to retain in terms of the Companies Act, must be retained for a period of 7 years even if a shorter period is specified in other legislation. For example, the Tax Administration Act requires that tax records be kept for 5 years. A company must keep its tax records for 7 years even though a shorter period is specified in the Tax Administration Act

29.4 Maximum period of retention

- 29.4.1 Where a statute imposes a maximum period of retention, we have highlighted this in the Code.
- 29.4.2 If a maximum period is stipulated in a statute, then, unless any exceptions apply, the record may not be retained beyond the maximum period of retention. This applies equally to companies who are ordinarily required to keep records for 7 years.
- 29.4.3 In terms of POPI, a record of personal information may be retained for longer than the maximum period if, amongst other things, a law requires that the record be retained for a longer. Unless one of the other POPI exceptions apply, once the minimum retention period expires, the record must be destroyed, deleted or the personal information de-identified

29.5 The Electronic Communications and Transactions Act

- 29.5.1 Following the commencement of ECATA, a record that was originally created in electronic form will be accepted as an original provided the electronic record satisfies the criteria of section 14 of ECATA.
- 29.5.2 The import of section 14 (set out in full below), is that all records created electronically, such as records of online transactions, books of account kept electronically, emails, text messages, digital photographs and electronic registers, will be regarded as “originals” if legislation requires that an original be retained.
- 29.5.3 Original electronic records, digitised records and records that have been converted from electronic format to another, that are retained in an electronic form, will satisfy an obligation to retain records in terms of legislation provided the requirements of section 16 of ECATA (set out in full below) are met.
- 29.5.4 Note that where an Act imposes an obligation to retain an original record and the original record is a paper record, the original paper record must be retained.
- 29.5.5 For example, a document containing the terms and conditions of an agreement can be created using word processing software. If the document is printed and signed by hand, the final form of the agreement that comes into existence upon signature is the hardcopy. The hand-signed hard copy is the original because this is the final form of the document. If the agreement is signed using electronic signatures, the electronic document will be regarded as the original provided it can be shown that the integrity of the document has been maintained during the period that it was retained electronically, and the document can be produced when required.
- 29.5.6 Sections 14 and 16 of ECATA are applicable to all record retention obligations contained in South African legislation. It is applicable to record retention obligations contained in legislation that does not expressly authorise electronic record keeping. It is also applicable to record retention obligations contained in legislation that predates ECATA.
- 29.5.7 The obligation to show that an electronic record meets the requirements of sections 14 and 16 rests on the person who is subject to the retention obligation. Documents that are stored and retained in a manner that reliably ensures their integrity will carry greater evidentiary weight¹.
- 29.5.8 ECATA defines “data” as meaning “electronic representations of information in any form”. It defines a “data message” as meaning “data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record”. ECATA commenced on 30 August 2002 and the term “data message” is now outdated and not commonly used.

29.6 Electronic record keeping obligations in terms of other legislation

- 29.6.1 Some statutes impose electronic record retention requirements that are over and above those contained in ECATA. Certain statutes prescribe where the records must be kept and specify what safeguards must be implemented to preserve the integrity of the electronic record.
- 29.6.2 The Companies Act specifically requires that accounting records that are kept electronically must be in a form that allows that information to be converted into written form in a “reasonable period of time”. It further requires that the company ensure that precautions specified in the Act are in place to safeguard is electronic accounting records and ensure the information’s integrity. A company must also ensure that the records are at all times capable of being retrieved to a “readable and printable form”. A company’s accounting records must be “accessible” from the company’s registered office².
- 29.6.3 In terms of the Consumer Protection Act, intermediaries must ensure that electronic records are “easily accessible” and “readily reducible to written or printed form”
- 29.6.4 Tax records may, in terms of the Tax Administration Act, be kept in electronic form provided the detailed requirements set out in the Notice on Electronic Form of Record Keeping³ (the “Electronic Form Notice”) are met. In terms of the Electronic Form Notice, tax records, including electronic tax records, must be kept at a place physically located in South Africa unless authorisation has been given to keep the records outside of South Africa. The provisions of the Electronic Form Notice do not preclude the maintenance of backup copies outside of South Africa.
- 29.6.5 Both the Tax Administration Act and sections of ECATA that deal with electronic transactions, require that particular records be kept of internet-based transactions and that safeguards be implemented.

29.7 Preserving the integrity of original electronic records and ensuring that electronic copies accurately represent the original record

- 29.7.1 If it is not self-evident from the record, separate records should be kept of the purpose for which, and circumstances in which, the record was created.
- 29.7.2 We recommend that detailed metadata⁴ be associated with the electronic records that reliably-
- 29.7.2.1 documents the identity of the originator;
 - 29.7.2.2 documents the manner in which the record was created, converted into electronic form, or converted from one form to another (as the case may be), as well as the safeguards that were in place at the time to preserve the integrity of the record;
 - 29.7.2.3 documents the origin and destination of an electronic record that has been sent or received, as well as the date and time that the electronic record was sent or received,

- 29.7.2.4 documents all processes performed on the record from the time that it was first created or converted into an electronic record until the end of its period retention,
 - 29.7.2.5 shows that the electronic record was not tampered with, or altered, in any way during the period of retention;
 - 29.7.2.6 preserves the record by preventing changes from being made; and
 - 29.7.2.7 restricts access to the record.
- 29.7.3 We also recommend that –
- 29.7.3.1 the electronic records be stored on a medium that is appropriate for long term retention;
 - 29.7.3.2 the electronic repository has sufficient storage capacity;
 - 29.7.3.3 archives and backups be securely maintained;
 - 29.7.3.4 separate records be kept with particulars of historical archives and backups;
 - 29.7.3.5 documented technical and organisational measures be instituted to safeguard against unauthorised access, theft, loss or intentional or accidental damage, destruction and falsification; and
 - 29.7.3.6 systems be implemented to facilitate the discovery of any attempted or actual changes, falsification or unauthorized access.
- 29.7.4 In order to give effect to the safeguards recommended above, steps should be taken to –
- 29.7.4.1 identify all reasonably foreseeable internal and external risks to records;
 - 29.7.4.2 establish and maintain appropriate safeguards against the risks identified;
 - 29.7.4.3 regularly verify that the safeguards are effectively implemented; and
 - 29.7.4.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

29.8 COMPANIES ACT 71 OF 2008

The Companies Act together with the Companies Regulations, 2011¹⁴ (referred to as the “Regulations” in the section) contain a number of retention requirements.

The general rule for the retention is contained in section 24 of the Act. In terms of this section, any documents, accounts, books, writing, records or other information that a company is required to keep in terms of this Act, or any other public regulation 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. The minimum period for which a company must retain records in terms of the Act, as well as other public regulation, is 7 years. This requirement applies even if a lesser period is specified in legislation other than the Companies Act.

If a maximum period of retention is specified in other public regulation, the shorter maximum period will prevail over the minimum 7-year period unless any exceptions to the maximum retention period apply.

If the original record is a paper record and this Act requires that an original be retained, the original paper record must be retained. If the original record is in electronic form, the record will be regarded as an original if the provisions of section 14 of ECATA are met.

Where this Act permits a copy to be retained, the copy may be retained in either paper or electronic form (which includes paper records that have been digitised). The retention requirement in the Act will be met if a record is retained electronically: provided the provisions of section 16 of ECATA are met.

If a paper document is digitised and retained electronically, a separate record should be kept showing how the integrity of the paper record, in its final form, was preserved prior to being digitised.

Note that this Act imposes specific retention requirements in respect of electronic accounting records over and above the requirements set out in ECATA.

Information forming part of electronic accounting records, must be in a form that allows the information to be converted into written form in a “reasonable time; and the precautions specified in section 24 must be in place to ensure the integrity of the records. Accounting records must be accessible from the registered office of the company. This requirement will be satisfied if electronic records are retained at another location, but which can still be accessed electronically from the registered office.

A company must notify the Companies and Intellectual Property Commission of the location, or of any change in the location, of any company records that are not located at, or accessible from, its registered office.

COMPANIES ACT 71 OF 2008

NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
1.	Memorandum of Incorporation including Amendments Section 24	Copy	Indefinitely	The Memorandum of Association and Articles of Association of a company incorporated prior to 1 May 2011 is included in the Act's definition of "Memorandum of Incorporation". The original Memorandum of Incorporation is filed with the Companies and Intellectual Property Commission.
2.	Company rules including any prior versions thereof Section 24	Copy	Indefinitely	
3.	Registration Certificate Section 24	Original	Indefinitely	

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
4.	Accounting records Sections 24 and 28 read with regulation 25	Original	7 completed financial years from the end of the financial year to which they relate as well as the then current financial year	<p>“Accounting records” are defined in the Companies Act as being information in written or electronic form concerning the financial affairs of a company as required in terms of the Act, including (but not limited to) purchase and sales records, general and subsidiary ledgers and other documents and books used in the preparation of financial statements.</p> <p>A company must keep accounting records in an official language of the Republic, as necessary to provide an adequate information base sufficient to-</p> <ol style="list-style-type: none"> 1. enable the company to satisfy all reporting requirements applicable to it in terms of the Act; and 2. provide for the compilation of financial statements, and the proper conduct of an audit, or independent review, of its annual financial statements, as applicable for the particular company. <p>The accounting records must include:</p> <ol style="list-style-type: none"> 1. A record of assets, which must include, but is not limited to <ol style="list-style-type: none"> a. current assets; b. non-currents assets showing for each asset (or groups of minor assets) – <ol style="list-style-type: none"> i. the date of acquisition and the acquisition cost; ii. if applicable, the date upon which the company was revalued, the amount of revaluation as well as the basis of, and reason for, the revaluation; iii. the date the company disposed of, or retired, the asset, the value of the consideration (if any) and the name of the person to whom it was transferred; and

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
				<ul style="list-style-type: none"> c. records of any loan by the company to a shareholder, director, prescribed officer or employee of the company, or to a person related to any of them, including the amount borrowed, the interest rate, the terms of repayment, and material details of any breach, default or renegotiation of any such loan. <p>2. A record of any liabilities and obligations, which must include, but is not limited to –</p> <ul style="list-style-type: none"> a. a record of any loan to the company from a shareholder, director, prescribed officer or employee of the company, or from a person related to any of them, including the amount borrowed, the interest rate, the terms of repayment, and material details of any breach, default or renegotiation of any such loan; and b. a record of any guarantee, suretyship or indemnity granted by the company in respect of an obligation to a third party incurred by a shareholder, director, prescribed officer or employee of the company, or by a person related to any of them, including the amount secured, the interest rate, the terms of re-payment, the expiry date, and the circumstances in which the company may be called upon to honour the guarantee, suretyship or indemnity. <p>3. Property records which must include, but are not limited to –</p> <ul style="list-style-type: none"> a. property held in a fiduciary capacity; and b. property held in terms of section 65(2) of the Consumer Protection Act (i.e. any prepayment, deposit, membership fee or other money or property belonging to a consumer that is in the possession of the company).

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
				<p>4. Records of revenue and expenditures which must include, but are not limited to –</p> <ul style="list-style-type: none"> a. daily records of money received and paid out; b. daily records of all good/services purchased or sold on credit; and c. statements of every account maintained at financial institutions together with vouchers or other supporting documents all transactions recorded on any such statement. <p>5. Stock records which must include, but are not limited to –</p> <ul style="list-style-type: none"> a. inventories and stock in trade, statements of annual stocktaking, and records to enable the value of stock at the end of the financial year to be determined; and b. non-profit companies must maintain records of revenue received from donations grants and member’s fees and in terms of funding contracts. <p>The location of accounting records</p> <p>A company’s accounting records must be kept at, or must be accessible from, the registered office of the company.</p> <p>Specific retention standards and safeguards for accounting records</p> <p>The accounting records required to be kept must be kept in such a manner as to provide adequate precautions against theft, loss or intentional or accidental damage or destruction and falsification. The manner in which the records are kept must also facilitate the discovery of any falsification.</p>

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
				<p>The accounting records must comply with any other applicable law dealing with accounting records, access to information, or confidentiality.</p> <p>Specific retention standards for electronic accounting records</p> <p>If a company keeps any of its accounting records in electronic form, the company must –</p> <ol style="list-style-type: none"> 1. provide adequate precautions against loss of the records as a result of damage to, or failure of, the media on which the records are kept; and 2. ensure that the records are at all times capable of being retrieved to a readable and printable form, including by converting the records from legacy to later systems, storage media, or software, to the extent necessary from time to time.
5.	Annual financial statements Sections 24 and 29	Original	7 years after the date that the annual financial statement was issued	
6.	Annual general meeting reports Section 24	Original	7 years after the date of the annual general meeting	

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
7.	Record of directors and past directors Section 24	Original	7 years after date the director ceased to be a director	The record must be maintained from the date that the person is appointed as a director. The record must include the following information: <ol style="list-style-type: none"> 1. full name, and any former names; 2. identity number; 3. nationality and passport number (if not South African); 4. occupation; 5. date of the person's last election or appointment as director of the company; and 6. name and registration number of every other company or foreign company of which the person was a director as at the date of retirement, and, in the case of a foreign company, the nationality of that foreign company.
8.	Notices and minutes of all shareholders meetings Section 24	Original	7 years after the date of the shareholders meeting	
9.	Resolutions adopted by shareholders and all documentation that was made available to shareholders in relation to each resolution Section 24	Original	7 years after the date of adoption of the resolution	
10.	All written communication to holders of securities Section 24	Original/copy*	7 years after the date of the communication	Proof of sending, delivery and receipt should be retained if available

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
11.	Minutes of meetings of directors, board committees or the audit committee Section 24	Original	7 years after the date of adoption	
12.	Resolutions of directors, board committees or the audit committee Section 24	Original	7 years after the date of adoption	
13.	Securities register and uncertificated securities register Section 24	Original	Indefinitely	
14.	Register of company secretary and auditors Section 24	Original	Indefinitely	
15.	Register of disclosures of persons who hold beneficial interest equal to or in excess of 5% of the securities of that class issued Section 56	Original	Indefinitely	This requirement is only applicable to regulated companies (i.e. Companies to which parts B and C of chapter 5 and the Takeover Regulations apply)

POPI Act – Code of Conduct

COMPANIES ACT 71 OF 2008				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
16.	Securities register and uncertified securities register Section 50	Original	Indefinitely	<p>A company must establish a register of its issued securities. In respect of each class of securities that it has issued it must specify the total number of those securities that are held in uncertified form.</p> <p>In respect of certified securities, the register must specify –</p> <ol style="list-style-type: none"> 1. the names and addresses of the persons to whom the securities were issued; 2. the number of securities issued to them; 3. the number of, and prescribed circumstances relating to, any securities – <ol style="list-style-type: none"> a) that had been placed in a trust; or b) his transfer has been restricted. <p>In the case of any debt instrument issued by the company, the securities register must reflect –</p> <ol style="list-style-type: none"> 1. the number of those securities issued and outstanding; and 2. the names and addresses of the registered owner of the security and any holders of beneficial interest in the security. <p>The register must also contain any information that may be prescribed by regulation from time to time.</p>

29.9 BASIC CONDITIONS OF EMPLOYMENT ACT 75 OF 1997 (BCEA)

The BCEA, together with the Regulations in Terms of Section 86(1), 199828 impose a number of record retention obligations on employers in respect of their employees.

The BCEA defines an employee as being –

(1) any person, excluding an independent contractor, who works for another person or for the State and who receives, or is entitled to receive, any remuneration;

And

(2) any other person who in any manner assists in carrying on or conducting the business of an employer.

If the original record is a paper record and this Act requires that an original be retained, the original paper record must be retained. If the original record is in electronic form, the record will be regarded as an original if the provisions of section 14 of ECATA are met. These provisions as well as a commentary thereon are set out at page 11 above under the heading “Good Electronic Record Keeping”.

Where this Act permits a copy to be retained, the copy may be retained in either paper or electronic form (which includes paper records that have been digitised). The retention requirement in the Act will be met if a record is retained electronically: provided the provisions of section 16 of ECATA are met. These provisions as well as a commentary are set out at page 11 above under the heading “Good Electronic Record Keeping”.

If a paper document is digitised and retained electronically, a separate record should be kept showing how the integrity of the paper record, in its final form, was preserved prior to being digitised.

The Act requires, in certain instances, that personal information be collected and retained. At the end of the minimum period of retention, any record of personal information must be destroyed, deleted or the personal information de-identified. If one of the other POPI exceptions apply, the record may be kept for longer.

Any record retained in terms of this Act, that is also required in order to comply with the provisions of a tax Act, must be retained for 5 years from the date specified in Tax Administration Act.

A company that is required to retain records in terms of this Act, must retain the records for a minimum period of 7 years.

BASIC CONDITIONS OF EMPLOYMENT ACT 75 OF 1997

NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
1.	Record of particulars of Employment Section 29(4)	Original	3 years after the date of termination of employment	<p>Written particulars of employment (which must be revised to reflect any changes) of the following must be retained by the employer:</p> <ol style="list-style-type: none">1. the full name and address of the employer;2. the name and occupation of the employee, or a brief description of the work for which the employee is employed;3. the place of work, and, where the employee is required or permitted to work at various places, an indication of this;4. the date on which the employment began;5. the employee's ordinary hours of work and days of work;6. the employee's wage or the rate and method of calculating wages;7. the rate of pay for overtime work;8. any other cash payments that the employee is entitled to;9. any payment in kind that the employee is entitled to and the value of the payment in kind;10. how frequently remuneration will be paid;11. any deductions to be made from the employee's remuneration;12. the leave to which the employee is entitled;13. the period of notice required to terminate employment, or if employment is for a specified period, the date when employment is to terminate;14. a description of any council or sectoral determination which covers the employer's business;15. any period of employment with a previous employer that counts towards the employee's period of employment; and16. a list of any other documents that form part of the contract of employment, indicating a place that is reasonably accessible to the employee where a copy of each may be obtained.

POPI Act – Code of Conduct

BASIC CONDITIONS OF EMPLOYMENT ACT 75 OF 1997				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
				<p>The last three record keeping requirements do not apply to employers who employ fewer than five employees.</p> <p>An employer need not keep the above records in respect of an employee who works less than 24 hours a month for an employer</p>
2.	Employee records Section 31 (a) –(d)	Original	3 years from the date of last entry in the record	<p>Each employer must keep a record containing following information:</p> <ol style="list-style-type: none"> 1. the employee’s name and occupation; 2. the time worked by each employee; 3. remuneration paid to the employee; and 4. the date of birth of any employee under 18 years of age.
3.	Wages register Section 31(e)) Regulation 3(1)(a) and Form BCEA 2	Original	3 years from the date of the last entry in the register	<p>An employer must maintain wages register in the form of BCEA 2 or some other record that contains the following information:</p> <ol style="list-style-type: none"> 1. name of employee; 2. identity number; 3. employee number; 4. pay period; 5. basic wage; 6. occupation; 7. the manner of payment - per hour/per day/per week/per fortnight/per month); 8. calculation of wages showing - <ol style="list-style-type: none"> a) ordinary hours worked and amount due; b) over time worked and amount due; c) hours worked on Sunday and amount due; 9. details and the value of any allowances for - <ol style="list-style-type: none"> a) shift; b) housing; c) transport; d) medical; and e) any other allowance afforded to the employee;

POPI Act – Code of Conduct

BASIC CONDITIONS OF EMPLOYMENT ACT 75 OF 1997				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
				10. authorised deductions in respect of – a) Pay-As-You-Earn (P.A.Y.E) b) Unemployment Insurance Fund (UIF) c) union dues; d) medical; e) retirement; f) other deductions (full details of which must be recorded); and g) total remuneration due.
4.	Attendance register Section 31(e) Regulation 3(1)(b) and Form BCEA 3	Original	3 years from the date of the last entry in the register	An employer must maintain an attendance register in the form of BCEA 3 or some other record that contains the following information in respect of each day worked: 1. the date and day of the week; 2. starting time; 3. meal intervals; 4. finishing time 5. total number of hours worked each day; 6. total number of hours worked each week; 7. start and end times of overtime worked; 8. total hours of overtime work; 9. start and end times of Sundays worked; 10. total time worked on Sundays; 11. start and end times of public holidays worked; and 12. total hours worked on public holidays.
5.	Learnership records	Original	3 years	Records must be retained in terms of the Skills Development Act. The records must contain the following information: 1. the learner’s name and learnership; 2. the time worked by each learner; 3. the remuneration paid to each learner; and 4. the date of birth of any learner under 18 years of age.

29.10 COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT 130 OF 1993

Recordkeeping and retention requirements are contained in the Act and in the Rules, Forms and Particulars Which Must be Furnished in Terms of the Compensation for Occupational Injuries and Diseases Act, 1993:29 (the "Rules").

If the original record is a paper record and this Act requires that an original be retained, the original paper record must be retained. If the original record is in electronic form, the record will be regarded as an original if the provisions of section 14 of ECATA are met.

Where this Act permits a copy to be retained, the copy may be retained in either paper or electronic form (which includes paper records that have been digitised). The retention requirement in the Act will be met if a record is retained electronically: provided the provisions of section 16 of ECATA are met.

If a paper document is digitised and retained electronically, a separate record should be kept showing how the integrity of the paper record, in its final form, was preserved prior to being digitised.

The Act requires, in certain instances, that personal information be collected and retained. At the end of the minimum period of retention, any record of personal information must be destroyed, deleted or the personal information de-identified. If one of the other POPI exceptions apply, the record may be kept for longer.

Any record retained in terms of this Act, that is also required in order to comply with the provisions of a tax Act, must be retained for 5 years from the date specified in Tax Administration Act.

A company that is required to retain records in terms of this Act, must retain the records for a minimum period of 7 years.

COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT 130 OF 1993

NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
1.	A register or other record of the earnings and other prescribed particulars of all the employees Section 81 and 82 Section 3 of the Rules and Form WAs.8	Original	4 years from date of last entry	<p>An employer, together with its payroll administrator, must submit a record of earnings in terms of section 82(1) of the Act. In terms of regulation 3 the Rules, the return must be on Form WAs.8 or submitted electronically. Based on the content of the form, the employer must keep a record of the following:</p> <ol style="list-style-type: none"> 1. particulars of the business operations; 2. status of the business; 3. number of employees and amount of earnings (staff costs/salaries and wages) per month paid to all employees (excluding directors of the company or members of a close corporation 4. number of directors /members and amount of earnings (staff costs /salaries & wages) per month paid to directors of a company or members of a close corporation up to a maximum of R403 500 per person for year; and 5. total cash value of free food and/or quarters.
2.	Records of accidents and occupational diseases* Section 39(1) and (5) Section 68(2)	Original/copy	4 years from date of last entry	<p>The Act does not require that an employer keep a record of accidents and occupational diseases although an employer is required to notify the Commissioner using the prescribed forms in the Rules. The particulars of the employee claiming compensation are required for the completion of the requisite forms as are particulars of the accident/occupational disease.</p> <p>Notwithstanding that there is no statutory requirement to retain records or the forms submitted to the Compensation Commissioner, it is nevertheless advisable to do so. Proof of submission should also be retained.</p>

29.11 LABOUR RELATIONS ACT 66 OF 1995 (LRA)

In the LRA, where an obligation is imposed to retain an original record, the legislation permits a “reproduced form” of the document to be retained. No definition is given in the Act or in any other legislation, but it is generally understood that the reproduction of a document is the process of creating copies from a source document and this would include electronic copies. It is recommended that if records are to be retained in their “reproduced form” a record also be kept to show that the integrity of the original document was preserved.

We have made some recommendations. These are marked with *If the original record is a paper record and this Act requires that an original be retained, the original paper record must be retained. If the original record is in electronic form, the record will be regarded as an original if the provisions of section 14 of ECATA are met.

Where this Act permits a copy to be retained, the copy may be retained in either paper or electronic form (which includes paper records that have been digitised). The retention requirement in the Act will be met if a record is retained electronically: provided the provisions of section 16 of ECATA are met.

If a paper document is digitised and retained electronically, a separate record should be kept showing how the integrity of the paper record, in its final form, was preserved prior to being digitised.

The Act requires, in certain instances, that personal information be collected and retained. At the end of the minimum period of retention, any record of personal information must be destroyed, deleted or the personal information de-identified. If one of the other POPI exceptions apply, the record may be kept for longer.

Any record retained in terms of the LRA, that is also required in order to comply with the provisions of a tax Act, must be retained for 5 years from the date specified in Tax Administration Act. A company that is required to retain records in terms of this Act, must retain the records for a minimum period of 7 years.

LABOUR RELATIONS ACT 66 OF 1995

NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
1. Records of bargaining councils Sections 53 and 54				
1.1	Accounting records	Original or Reproduced form	3 years from the end of the financial year to which they relate	These records must include: 1. books of account recording income, expenditure, assets and liabilities; 2. supporting vouchers, 3. income and expenditure statements, and 4. balance sheets.
1.2	Audited financial statements and auditors' reports	Original or reproduced form	3 years from the end of the financial year to which they relate	
1.3	Records of investments	Original or Reproduced form	3 years from date of creation of the record	A separate record should be kept of funds that have been invested to show compliance with section 53(5)
1.4	Minutes of meetings	Original or Reproduced form	3 years from the date of adoption	
1.5	Records regarding small enterprises	Original or reproduced form	3 years from the date of last entry*	In order to report to the Commission for Conciliation, Mediation and Arbitration (CCMA) in terms of section 54(2)(f), councils should keep records of the following: 1. the number of employees who are employed by small enterprises that fall within the registered scope of the council, and the number of employees of those enterprises who are members of trade unions; 2. the number of employees employed by small enterprises that are covered by a collective agreement that was concluded by the council and extended by the labour minister in terms of section 32; 3. the number of small enterprises that are members of the employers' organisations that are parties to the council; and

POPI Act – Code of Conduct

LABOUR RELATIONS ACT 66 OF 1995				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
				<p>4. the number of applications for exemptions received from small enterprises, the number of applications that were granted and the number rejected.</p> <p>It is not a requirement that the records be retained but it is advisable to do so. Proof of submission of reports to the CCMA should be retained.</p>
1.6	Collective Agreements*	Original or copy	3 years from date of termination*	Certified copies of collective agreement must be submitted to the CCMA. The Act does not oblige councils to retain copies of collective agreements that it submits to the CCMA. Nevertheless, it is advisable to retain copies.
1.7	Records of admission and resignation of parties to the council	Original	3 years from date of termination*	A council is required to inform the CCMA of all admissions and resignations. A council is not obliged to keep records, but it is nevertheless advisable to do so.
2	Records of registered trade unions and registered employers' organisations Section 98, 99, and 100			
2.1	Accounting records	Original or Reproduced form	3 years from the end of the financial year to which they relate	<p>These records must include:</p> <ol style="list-style-type: none"> 1. books of account; 2. supporting vouchers; 3. records of subscriptions or levies paid by its members; 4. income and expenditure statements; and 5. balance sheets.
2.2	Audited financial statements and auditors' reports	Original or Reproduced form	3 years from the end of the financial year to which they relate	
2.3	List of members	Original or Reproduced form	3 years from date of last entry*	The LRA requires that the records be kept but does not specified a retention period.

POPI Act – Code of Conduct

LABOUR RELATIONS ACT 66 OF 1995				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
2.4	Minutes of meetings	Original or Reproduced form	3 years from the date of adoption	
2.5	Ballot papers	Original	3 years from the date of the ballot	
2.6	Records of office bearers	Original	3 years from date of last entry*	<p>The Act requires that the Registrar of Labour Relations be informed of any appointment or election of its national office bearers, as well as the names and works addresses of those office bearers. Proof that such information has been conveyed should be retained.</p> <p>The Act does not require that a record be retained. Nevertheless, it is advisable to do so.</p>
2.7	Constitution and amendments thereto	Original/copy	* Period of validity *	Whilst it is not a requirement of the Act that a copy be retained it is nevertheless advisable to do so
3.	Records of employers			
3.1	Records in terms of collective agreements, arbitration awards, and determinations made in terms of the Wage Act Section 205(1) LRA Form 9.1	Original or Reproduced form	3 years from the date of the event or the end of the period to which they relate	Every employer must retain records that it is required to keep in compliance with the terms of any applicable collective agreement, arbitration award or determination made in terms of the Wage Act. In terms of the Labour Relations Regulations, 2014 ³⁰ the records must include a record of employees' earnings, deductions and times worked.

POPI Act – Code of Conduct

LABOUR RELATIONS ACT 66 OF 1995				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
3.2	Records of strikes, lockouts or protest action involving Employees Section 205(3) LRA Form 9.2	Original	3 years from the date of the event*	<p>The Act does not specify a period of retention but it is nevertheless advisable to retain the record.</p> <p>The employer must complete and submit LRA Form 9.2 which must contain the following details from the employers' records:</p> <ol style="list-style-type: none"> 1. details of the employees; 2. details of the action; 3. particulars of any lockout; 4. duration of the strike; 5. unions involved; 6. numbers of employees participating and affected; 7. total work hours lost; 8. total wages not paid; and 9. reasons for the strike.
3.3	Disciplinary action Schedule 8, section 5	Original	3 years from date of termination of employment*	<p>An employer must keep records for each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions.</p> <p>The LRA does not specify a period of retention but it is nevertheless advisable to retain the record.</p>

29.12 UNEMPLOYMENT INSURANCE ACT, NO 63 OF 2002

If the original record is a paper record and this Act requires that an original be retained, the original paper record must be retained. If the original record is in electronic form, the record will be regarded as an original if the provisions of section 14 of ECATA are met. Where this Act permits a copy to be retained, the copy may be retained in either paper or electronic form (which includes paper records that have been digitised). The retention requirement in the Act will be met if a record is retained electronically: provided the provisions of section 16 of ECATA are be met.

If a paper document is digitised and retained electronically, a separate record should be kept showing how the integrity of the paper record, in its final form, was preserved prior to being digitised.

The Act requires, in certain instances, that personal information be collected and retained. At the end of the minimum period of retention, any record of personal information must be destroyed, deleted or the personal information de-identified. If one of the other POPI exceptions apply, the record may be kept for longer. A company that is required to retain records in terms of this Act, must retain the records for a minimum period of 7 years.

UNEMPLOYMENT INSURANCE ACT, NO 63 OF 2002				
NO	RECORD	ORIGINAL / COPY	MINIMUM PERIOD OF RETENTION	COMMENTS
1.	Employers' records in respect of contributors Regulation 8(2)	Original	5 years from the date of last entry	Every employer shall keep, in respect of every contributor, a record showing- <ol style="list-style-type: none"> 1. the name of such contributor; 2. the date upon which such contributor commenced employment with him as a contributor; 3. the date upon which his employment as a contributor terminated; 4. the weekly or monthly rate of earnings of such contributor during the 13 weeks immediately preceding the date of termination of such employment; 5. the date upon which the employer received the contributor's record card (UF 74) of such contributor from the said contributor, or from the Director- General, as the case may be; 6. the date upon which the employer disposed of such contributor's record card and the manner of such disposal

29.13 ELECTRONIC STORAGE

The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned

Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years, must be retained for a period of 3 years after termination of employment

Section 51 of the Companies Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

29.14 DESTRUCTION OF DOCUMENTS

Documents may be destroyed after the termination of the retention periods listed above. The Company will attend to the destruction of their documents and will be attended to as soon as possible.

The Company is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file.

After completion of the process, the Information Officer shall in writing authorise the removal and destruction of the documents in the authorisation document. These records will be retained by registration.

The documents will then be shredded before disposal. This also helps to ensure confidentiality of information.

Documents may also be stored off-site, in storage facilities approved by the Company.

29.15 SHREDDING POLICY

All office documents and paper, and other sensitive media with personal information must be secured and shredded according to Company policy. All sensitive and items perceived as sensitive material must be secured for shredding.

Workflow Procedure

1. All office paper and documents are deposited into the designated containers located in each office.
2. Conveniently placed security containers will allow for easy access for all employees.
3. Paper must be separated from items that are not considered critical. Items that should not be placed into the containers includes, but is not limited to, newspapers, magazines, boxes, cardboard, plastics (covers, for example), 3-ring binders (remove paper for shredding), wrappings, etc
4. Items that are OK include: all office paper (paper clips, rubber bands, staples are fine), file folders, coloured office paper, and more.
5. Larger volume needs can be addressed easily.

Proper adherence to these instructions will help with a compliance policy for document management and destruction, and will reduce risk of personal information being protected. The shred policy is intended as a responsibility of each employee.

Unless instructed to the contrary by the Regulator, as soon as reasonably possible, notify the data subject of its knowledge or suspicion that the data subject's personal information has been accessed or acquired by an unauthorised person.

PART D – INFORMATION OFFICER, DIRECT MARKETING AND TRANSBORDER INFORMATION FLOWS

30. INFORMATION OFFICER

31. COMPANY INFORMATION OFFICER

The details of The Company's Information Officer, Deputy Information Officer and Head Officer are as follows:

INFORMATION OFFICER:

Name and Surname: Sunelle du Toit
Telephone Number: 0829024466
Email Address: chairman@willowacres.co.za

DEPUTY INFORMATION OFFICER:

Name and Surname: Elana Goodwin
Telephone Number: 0823297024
Email Address: manager@willowacres.co.za

HEAD OFFICE DETAILS

Telephone Number: 0128091955
Postal Address: PO Box 201, Willow Acres Estate, 0095
Physical Address: 1 Hoopoe Crescent, Willow Acres, 0081
Email Address: admin@willowacres.co.za
Website Address: www.willowacres.co.za

31.1 DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER

An information officer's responsibilities include:

- a. the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;
- b. dealing with requests made to the body pursuant to this Act;
- c. working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;
- d. otherwise ensuring compliance by the body with the provisions of this Act; and
- e. as may be prescribed.

31.2 Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

31.3 DESIGNATION AND DELEGATION OF DEPUTY INFORMATION OFFICERS

Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of:

- a. Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and
- b. Any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

31.4 OTHER APPLICABLE LEGISLATION:

The Promotion of Access to Information Act, 2 of 2002 ("PAIA"):

- a. PAIA, in relation to a private body, defines the head of a juristic person as the chief executive officer or equivalent officer of the juristic person, or any person duly authorised by the Chief Executive Officer.
- b. In terms of PAIA it is the head or a person delegated by the head who acts on behalf of the organisation in fulfilling the organisation's obligations to provide access to records of the organisation;
- c. PAIA will, on the commencement of the Act, fall to be regulated by the Information Regulator appointed in terms of PoPIA.

- 31.5 An Information Officer is defined in relation to a private body, which is a juristic person, as either the Chief Executive (or equivalent) Officer or the person duly authorised by the Chief Executive (or equivalent) Officer.
- 31.6 In the case of the Company unless the Chief Executive (or equivalent) Officer has appointed an Information Officer, the Chief Executive (or equivalent) Officer will be deemed to be the Information Officer.
- 31.7 PoPIA also stipulates that information officers must take up their duties only after the responsible party has registered them with the Regulator.

32. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATION AND AUTOMATED DECISION-MAKING

32.1 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 machines, SMSs or e-mail is prohibited unless the data subject:

- a. has given his, her or its consent to the processing; or
- b. is, subject to subsection (3), a customer of the responsible party.

32.2 A responsible party may approach a data subject:

- a. whose consent is required; and
- b. who has not previously withheld such consent, only once in order to request the consent of that data subject?

32.3 The data subject's consent must be requested in the prescribed manner and form.

32.4 A responsible party may only process the personal information of a data subject who is a customer /client/employee of the responsible party:

- a. if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
- b. for the purpose of direct marketing of the responsible party's own similar products or services; and
- c. if the data subject has been given 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:
 - i. at the time when the information was collected; and
 - ii. on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

32.5 Any communication for the purpose of direct marketing must contain:

- a. details of the identity of the sender or the person on whose behalf the communication has been sent; and
- b. an address or other contact details to which the recipient may send a request that such communications cease.

32.6 “Automatic calling machine”, for purposes of subsection 21.1, means a machine that is able to do automated calls without human intervention.

32.7 Other Applicable Legislation:

The Consumer Protection Act, 68 of 2008 (“CPA”):

- The CPA deals relatively extensively with the right to fair and responsible marketing. This relates to all marketing of whatever nature and is not confined, as is the case with PoPIA, to direct marketing using electronic communications.
- The CPA deals with direct marketing to consumers in Section 32. This stipulates that where, as a result of direct marketing, a transaction is concluded for goods and services the consumer must be informed of the right to rescind the agreement. Further, that if any goods are left with the consumer without payment being made, the goods are to be considered unsolicited goods.

32.8 The principles governing direct marketing by means of unsolicited electronic communications are straightforward. There is no restriction on direct marketing by electronic communication to existing customers, provided that the customer is afforded the opportunity of opting out of further communications with the responsible party.

32.9 Where the data subject is not a customer, consent to the processing of personal information for the purposes of direct marketing (opt in) is required. The responsible party is entitled to approach the data subject for consent to direct marketing in electronic communications unless such consent has previously been withheld. If the person approached does not expressly agree to receipt of further electronic communications (opt in), any further communications to that person will be unlawful.

32.10 In terms of the Company the purpose of the processing of confidential information relates expressly to the provision of services that fall within the scope of the operations of the Company. If this information is used for another purpose such as direct marketing, this would be in breach of the Further Processing Limitations and unlawful.

32.11 Automated decision making:

32.11.1 A data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its reliability, location, health, personal preferences or conduct.

32.11.2 The provisions of subsection 21.11.1 do not apply if the decision—

- a. has been taken in connection with the conclusion or execution of a contract, and:
 - i. the request of the data subject in terms of the contract has been met; or
 - ii. appropriate measures have been taken to protect the data subject's legitimate interests;
- or
- b. is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

32.11.3 The appropriate measures, referred to in subsection 22.11.2 a. ii., must:

- a. provide an opportunity for a data subject to make representations about a decision referred to in subsection 22.11.1; and
- b. require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a).

32.12 Other Applicable Legislation:

32.12.1 The prohibition against automated decision making in the context of the operations of the Company, provided that a decision which may result in legal consequences for a data subject has been taken in connection with the conclusion or execution of a contract, and either:

- a. The request of the data subject in terms of the contract has been met; or
- b. Appropriate measures are in place to protect the data subject's legitimate interests in so far as automated decision making is concerned.

32.12.2 The protection of the legitimate interests of a data subject in this Code of Conduct is stipulated in Section 60(4)(a)(ii).

32.12.3 In addition to the reference to the protection of legitimate interests of data subjects in Section 71(2)(b) of PoPIA, the issue of legitimate interests of a data subject is addressed elsewhere in PoPIA.

32.12.4 Section 11(1) (dealing with the justification for the processing of personal information) stipulates that processing of personal information is lawful if it is:

- a. Legitimate interests of the data subject;
- b. Legitimate interests of the responsible party or of a third party to whom information is supplied;
- c. Dealing with the collection of information directly from a data;
- d. subject) provides that collection from another source is permissible if:
 - i. The collection would not prejudice the legitimate interest of the data subject; and
 - ii. Collection from another source is necessary to maintain the legitimate interests of the responsible party, or of a third party to whom the information is supplied.
- e. In many instances the legitimate interests of both the data subject on the one hand or a responsible party or third party on the other, would coincide. However, this is not always the case and the necessity exists to balance the legitimate interests of the data subject with that of the responsible party or a third party.
- f. In considering this balance it will always be necessary to take cognizance of the constitutional rights entrenched in the Bill of Rights of our Constitution. These rights are not absolute and any limitation to these rights have to be considered by taking into account the nature of the right, the important of the purpose of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose and whether there are less restrictive means of achieving the purpose.
- g. Against this background where automated decision making is employed in the processing of personal information, a responsible party must, in protecting the legitimate interests of the data subject:
 - i. Notify the data subject in terms of Section 18(1) that the processing of personal information may be subject to automatic decision making;
 - ii. Provide to the data subject sufficient information about the underlying logic of the automated decision-making technologies and processes to enable the data subject to make representations relating to the decision automatically made;
 - iii. Allow the data subject a reasonable opportunity for him or her to make representations to the responsible party about the decision.

33. TRANSBORDER INFORMATION FLOWS

33.1 A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless:

- a. the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:
 - i. effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and
 - ii. includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country.
- b. the data subject consents to the transfer;
- c. the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- e. the transfer is for the benefit of the data subject, and:
 - i. it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
 - ii. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

33.2 For the purpose of this section:

- a. "binding corporate rules" means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

- b. “group of undertakings” means a controlling undertaking and its controlled undertakings.

33.3 The purpose of prohibiting the transfer of personal information to a foreign country is straightforward. If the foreign country does not have adequate protection of personal information the possibility exists that the personal information (information knowing no borders) may be processed in a manner that violates the data subject’s right to privacy, including the right to determine the use of his or her personal information.

33.4 It is a feature of data protection legislation globally that unless the equivalent protection is provided in the foreign country, the transfer of the personal information to that country is prohibited, alternatively allowed subject to the fulfilment of conditions aimed to promote the protection of the personal information, regardless of the fact that there may be insufficient or inadequate laws in doing so in the foreign country.

PART E – ENFORCEMENT

34. INTERPRETATION OF POPIA AND THIS CODE OF CONDUCT

34.1 For the purposes of the interpretation of PoPIA and this Code of Conduct as well as the enforcement of PoPIA and this Code of Conduct “business days” shall mean all weekdays which are not proclaimed public holidays in the Republic of South Africa.

34.2 The Company or Executive Manager shall, for the purposes of this Part D of the Code of Conduct, include any person assigned by the Executive Manager to discharge the Executive Manager’s stipulated duties.

34.3 Consumers or Data Subjects

34.3.1 If customers/clients or data subjects (as defined in PoPIA) wish to complain about the conduct of the Company, PoPIA or this Code of Conduct the data subject must refer the complaint to the Company or the Information Regulator, as may be appropriate.

34.3.2 If a data subject is aggrieved with the actions of the Company on the grounds that they are contrary to this Code of Conduct, the complaint must be made to the Company or Information Regulator, as may be appropriate.

34.4 Interpretation and disputes relating to the Code of Conduct:

34.4.1 If a customer/client/employee of the Company wishes to request an interpretation of the Code of Conduct, the employee may address the request or complaint in writing to the Executive Manager of the Company.

34.4.2 If the request cannot be resolved by the Company Executive Manager it will be placed on the agenda for discussion at the next meeting of Management meeting.

34.4.3 If, at the Management meeting, a request or a complaint cannot be resolved by the members attending the meeting, the Company Executive Manager must refer the request or complaint to the Company Executive Committee.

34.4.4 The Company Executive Committee may, in its discretion:

- a. Make a decision and communicate the decision by email to its nominated representatives; or

- b. Refer the request or complaint to legal counsel for consideration and opinion; or
 - c. Recommend to the party requesting the interpretation or making the complaint to, at their own cost, obtain an opinion from legal counsel and provide this to the Executive Manager.
- 34.4.5 Once advice or an opinion has been obtained from legal counsel the Executive Manager will circulate this to the Executive Committee with a view to resolving the request or complaint.
- 34.4.6 If the party remains aggrieved by the advice or opinion from legal counsel, they may request the Company Executive Manager to again refer the matter to the Executive Committee, which may, but is not obliged to, appoint an independent adjudicator to consider and determine the request or complaint.
- 34.4.7 Nothing in this Code of Conduct prevents anyone from obtaining independent advice or opinion from legal counsel or a subject matter expert, as may be appropriate and providing this to the Executive Committee.

PART F – ADMINISTRATION OF CODE OF CONDUCT

35. COMPLIANCE WITH CHAPTER 7 OF POPIA

- 35.1 This Code of Conduct applies to the Company.
- 35.2 The Company has to apply to the Information Regulator for the issue of this Code of Conduct.
- 35.3 The Code of Conduct incorporates the conditions for the lawful processing of personal information and provides functional equivalence of obligations set out in those conditions that are applicable to the operations of the Company.
- 35.4 This Code of Conduct specifies appropriate measures for protecting the legitimate interests of data subjects with regard to “Automated Decision Making” in Part C.
- 35.5 This Code of Conduct will be reviewed by the Company within 1 (one) year of its coming into force in terms of Section 62(2) of PoPIA.
- 35.6 Further reviews of this Code of Conduct will be conducted annually by no later than the anniversary of the date of the coming into force of this Code of Conduct.
- 35.7 The review of this Code of Conduct may be accelerated:
- 35.7.1 if an earlier review is prescribed by the Regulator in writing addressed to the Company Executive Manager; or
 - 35.7.2 required in terms of a ruling made by the Regulator; or
 - 35.7.3 if directed to do so by the Regulator in an Information Notice issued in terms of Section 90 or an Enforcement Notice issued in terms of Section 95 of PoPIA; or
 - 35.7.4 if any court having jurisdiction over the Company who is a member of the COMPANY directs that any provisions of this Code of Conduct are unlawful.
- 35.8 The COMPANY will revoke or make any amendments to the Code of Conduct as directed by the Regulator, in compliance with Sections 60 to 63 of PoPIA.
- 35.9 This Code of Conduct will continue to be of force and effect indefinitely, subject to the Regulator’s direction as to the date of its expiry or termination by the Company.

- 35.10 On the termination of this Code of Conduct all employees of the Company will remain subject to the provisions of PoPIA and any other applicable laws governing the processing of personal information.
- 35.11 From the date that the Code of Conduct comes into force the Company will cause publication of the Code on its website.
- 35.12 The Company will make copies of the Code available in hardcopy form to persons requesting a copy in that form.
- 35.13 The interpretation of PoPIA and of this Code of Conduct as they relate to the operation of the Company may be made by the Company Executive Manager. No interpretation made by the Company Executive Manager shall be binding on the Information Regulator or detract from any of the powers of the Information Regulator stipulated in Chapter 10 of PoPIA.
- 35.14 The Company Executive Manager will ensure that a revision history of this Code of Conduct will be established and maintained.
- 35.15 The revision history must record the material aspects of any decisions or rulings made by the Regulator or by the Company Executive Committee that cause amendments to be made to this Code of Conduct.

36 SOURCES

- Companies Act 71 of 2008
- Basic Conditions of Employment Act No. 75 of 1997
- Employment Equity Act No 55 of 1998
- Unemployment Insurance Act
- Compensation for Occupational Injuries & Diseases Act
- Labour Relations Act No 66 of 1995
- The Occupational Health and Safety Act No. 85 of 1993
- POPI
- Legal Advice – AJ van Rensburg
- HR Assistance – Pretty Much People

37 APPENDIXES

FORM C



J752

REPUBLIC OF SOUTH AFRICA

FORM C
REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))
[Regulation 10]

A. Particulars of private body

The Head:

[Redacted area for Particulars of private body]

B. Particulars of person requesting access to the record

- (a) The particulars of the person who requests access to the record must be given below.
- (b) The address and/or fax number in the Republic to which the information is to be sent must be given.
- (c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname: [Redacted]

Identity number: [Redacted]

Postal address: [Redacted]

Telephone number: (.....) [Redacted] Fax number: (.....) [Redacted]

E-mail address: [Redacted]

Capacity in which request is made, when made on behalf of another person:
[Redacted]

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname: [Redacted]

Identity number: [Redacted]

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

D. Particulars of record

- (a) Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
- (b) If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of record or relevant part of the record:

.....

.....

.....

.....

2. Reference number, if available:

.....

.....

.....

.....

3. Any further particulars of record:

.....

.....

.....

.....

E. Fees

- (a) A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
- (b) You will be notified of the amount required to be paid as the request fee.
- (c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.
- (d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

.....

.....

.....

.....

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability: Form in which record is required:

Mark the appropriate box with an X.

NOTES:
 (a) Compliance with your request for access in the specified form may depend on the form in which the record is available.
 (b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
 (c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:					
<input type="checkbox"/>	copy of record*	<input type="checkbox"/>	inspection of record	<input type="checkbox"/>	<input type="checkbox"/>
2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):					
<input type="checkbox"/>	view the images	<input type="checkbox"/>	copy of the images*	<input type="checkbox"/>	transcription of the images*
3. If record consists of recorded words or information which can be reproduced in sound:					
<input type="checkbox"/>	listen to the soundtrack (audio cassette)	<input type="checkbox"/>	transcription of soundtrack* (written or printed document)	<input type="checkbox"/>	<input type="checkbox"/>
4. If record is held on computer or in an electronic or machine-readable form:					
<input type="checkbox"/>	printed copy of record*	<input type="checkbox"/>	printed copy of information derived from the record*	<input type="checkbox"/>	copy in computer readable form* (stiffy or compact disc)

*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES <input type="checkbox"/>	NO <input type="checkbox"/>
--	------------------------------	-----------------------------

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form.
The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

.....

Signed at this day..... ofyear

.....
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE

ANNEXURE 2 – FEES PAYABLE

PART III
FEES IN RESPECT OF PRIVATE BODIES

The fee for a copy of the manual as contemplated in terms of Regulation 9(2)(c) for every A4 size page or part thereof	1.10
The fee for reproduction referred to in Regulations 11(1) are as follows:	1.10
(a) For every photocopy of an A4 size page or part thereof	
(b) For every printed copy of an A4 size page or part thereof held on a computer in electronic or machine readable form	0.75
(c) For a copy in a computer-readable form on:	
(i) Stiffy disk	7.50
(ii) Compact disk	70.00
(d) For a copy of visual images:	
(i) for a transcription of visual images for an A4 sized page or part thereof	40.00
(ii) for a copy of visual images	60.00
(e) (i) For a transcript of an audio record for an A4 size page or part thereof	20.00
(ii) For a copy of an audio record	30.00
The request fee payable by a requester, other than a personal requester, referred to in Regulation 11(2)	50.00
The access fee payable by a requester referred to in regulation 11(3) are as follows:	
(a) For every photocopy of an A4 size page or part thereof	1.10
(b) For every printed copy of an A4 size page or part thereof held on a computer or in electronic of machine readable form	0.75
(c) For a copy in a computer-readable form on:	
(i) stiffy disk	7.50
(ii) compact disk	70.00
(d) For a copy of visual images:	
(i) for a transcription of visual images for an A4 sized page or part thereof	40.00
(ii) for a copy of visual images	60.00
(e) (i) For a transcript of an audio record for an A4 size page or part thereof	20.00
(ii) For a copy of an audio record	30.00
To search for an prepare the record for disclosure, for each hour or part of an hour reasonably required for such searches and preparation	30.00
For purposes of Section 54(2) of the Act, the following applies:	
(a) Six hours as the hours to be exceeded before a deposit payable; and	
(b) one third of the access fee is payable as a deposit by the requester	

The actual postage is payable when a copy of a record must be posted to a requester

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETING OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017
(Regulation 3 (2))**

Note:

1. *Affidavits or other documentary evidence in support of the request must be attached*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

Reference Number

Mark the appropriate box with an “x”

Request for:

Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT	
Surname:		
Full Names:		
Identity Number:		
Residential, postal or business address:	Code ()	
Contact number(s):		
Fax number:		
E-mail address:		
B	DETAILS OF RESPONSIBLE PARTY	
Name and Surname of Responsible Party (if the responsible party is a natural person)		
Residential, postal or business address:	Code ()	
Contact number(s):		
Fax number:		
E-mail address:		

POPIA COMPLIANCE OFFICER
Willow Acres Estate Homeowners Association NPC

CERTIFICATE OF APPOINTMENT

_____ as Chairperson of Willow Acres Estate Homeowners Association NPC confirm that I will act as the POPIA COMPLIANCE OFFICER

The purpose of this appointment is to give effect to; the right to privacy in terms of our common law, section 14 of the Constitution and the purpose and application of the Protection of Personal Information Act, No 4 of 2013.

Specifically, to implement and maintain the provisions of the POPI Act including but not limited to the following:

- To give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party.
- To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards that prescribed the minimum threshold requirements for the lawful processing of personal information.
- To provide persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act.

The Act regulates how anyone who processes personal information must be handle, keep and secure the information. If an individual or a company processes personal information relating to a person, that individual or company must comply with the Act. Failure to comply with the Act may lead to the imposition of certain penalties under the Act.

Punishable offences in terms of the Act. The following are, if committed, punishable with either a fine (not exceeding R10 million) or imprisonment (for a period not exceeding 10 years), or both:

- Obstruction of a regulator
- Failure to comply with enforcement or information notices
- Offences by witnesses – Giving false evidence before the Regulator
- Unlawful acts by a responsible party in connection with information / usage
- Unlawful acts by third parties in connection with information / usage
- Any person who sells/offers to sell information obtained illegally
- Failure to notify the Regulator that processing is subject to prior authorization.
- Breach of confidentiality
- Obstruction of the execution of a warrant.

Signature
Sunelle du Toit