	Does your company have PAIA manual?		
	Are your clients aware of all their rights?		
7	**SAFETY SAFEGUARDS**		
	Does your company provide safeguards to the clients in respect of the integrity and confidentiality of the personal information you have received?		
	Does the company have reasonable technical measures in place to prevent any loss and unlawful access to the personal information?		
	Does the company have sufficient protection on any and all software and access to electronic information?		
	Does the company have sufficient security measures in place to prevent access to personal information on their system?		
	Does the company have sufficient safety measures in place for protection of the data?		
	Does the company store any hard copies of personal information on site?		
	Does the company have measures to control access to such hard copies?		
	Does the company have control measures and security to control such access?		
	Has the company identified all internal and external risks?		
	Does the company maintain appropriate safeguards?		
	Does the company do regular safeguard checks and compliance checks?		
	Does the company have a process to follow in the event that data has been compromised?		
	Does the company have a process to inform their clients that data has been compromised however preventative measures have been taken?		
	Does the company have an Information Officer?		
	Does the company have a Deputy Information Officer as is required by PAIA?		
8	**DATA SUBJECT PARTICIPATION**		
	Does the company provide access to their clients to establish whether any personal information is being held by them?		
	Does the company have a required fee in the event that a client requests such information?		
	Does the company have a process to follow to update such personal information where clients have declined to update such personal information?		
	Does the company have a process to inform their clients that changes to their personal information was made?		

PROTECTION OF PERSONAL INFORMATION ACT POLICY AND PAIA MANUAL OF THE COMPANY

1. INTRODUCTION

This POPIA Act Policy and PAIA Manual describes the manner in which the company will meet its legal obligations and requirements concerning confidentiality, information security standards and access to information. The requirements within this policy are based upon the Protection of Personal Information Act, No 4 of 2013 and the Promotion of Access to Information Act, No 2 of 2000.

2. APPLICATION

The company needs personal information relating to both individual and juristic persons in order to carry out its business and organisational functions. The manner in which this information is processed and the purpose for which it is processed is determined by this manual. The company is, accordingly, the "responsible party" as defined in the POPIA and the company herewith further ensures that:

2.1 the data is processed lawfully, fairly and transparently;
2.2 the data is processed for the purpose for which it is collected;
2.3 the data will not be processed for a secondary purpose unless that processing is compatible with the original purpose;
2.4 the data is adequate, relevant and not excessive for the purpose for which it is collected;
2.5 the data is accurate and kept up to date;
2.6 the data will not be kept for longer than is necessary;
2.7 the data is processed in accordance with integrity and confidentiality principles, including physical and organisational measures to ensure that the personal information is both in physical and electronic form and are subject to appropriate levels and are subject to appropriate levels of security when stored, used and communicated by the company;
2.8 is processed in accordance with the rights of the customers, where applicable;
2.9 the customers have the right to be:
   a) notified that their personal information has been collected;
   b) notified that the data has been breached;
   c) know whether the company holds personal information about them and to access that information;
   d) request the correction or deletion of information which may be out of date, incomplete, misleading or unlawfully obtained;
   e) object to the company's use of their personal information;
   f) object to the processing of personal information for purposes of direct marketing;
   g) complain to the Information Regulator regarding infringements of any right protected under the POPIA Act and institute civil proceedings regarding the non-compliance with the protection of their personal information.

3. PURPOSE OF PROCESSING OF PERSONAL INFORMATION

Our customer's personal information may only be processed for specific purposes as set out herein.

CONSUMERS	Operate and manage consumers' accounts and manage any application, agreement or correspondence consumers may have with the company
	Communicating (including direct marketing) with consumers by email, SMS, letter, telephone or any other way in which the company wishes to inform clients of their products and services.
	Make or assist in making any credit decisions about consumers.
	Performing duties in terms of any agreement with consumers.
	To form a view of consumers as individuals and to identify, develop or improve product that may be of interest to consumers.
	Carry out market research, business and statistical analysis.
	Recovering any debt consumers may owe to the company complying with the company's regulatory and other obligations, performing any administrative and operational purposes including the testing of systems.
	Any other reasonably required purpose relating to the company's business.
EMPLOYEES	Contact details
	Employment history
	Refences
	Vetting information
	Financial information including banking details
	IT information
	General matters relating to employees; pension and medical aid
	Any other reasonably required purpose relating to the employment or possible employment relationship
SUPPLIERS	Verifying information and performing checks
	Purposes related to the agreement or business relationship or possible agreement or business relationship between the parties.
	Payment of invoices
	Complying with the company's regulatory and other obligations.
	Any other reasonably required purpose relating to the company's business.

4. CATEGORIES OF CUSTOMERS (DATA SUBJECTS AND PERSONAL INFORMATION)

EMPLOYEES	Name & contact details
	Identity documents, including passports, employment history and references
	Banking and financial details
	Details of payment to third parties (deductions from salary)
	Employment contracts, employment equity plans
	Medical Aid Records
	Pension Fund Records
	Remuneration Salary Records
	Performance Appraisals
	Disciplinary Records
	Leave Records
	Training Records
CONSUMERS OR PROSPECTIVE CONSUMERS	Postal and/or street address
	Title and name
	Contact numbers and email addresses
	Ethnic group
	Emp history
	Age
	Gender
	Marital status
	Nationality
	Language
	Financial information
	Identity or passport number
SUPPLIERS	Name and contact details
	Identity and/or company information and directors' information
	Banking and financial information
	Information about their products or services
	Other information not specified and reasonably required to be processed for the company's business operations.

5. RECIPIENTS OF PERSONAL INFORMATION

The company herewith confirms that personal information will be shared as follows:

5.1 any firm, organisation or person that the company uses to collect payments and recover debts or to provide a service on its behalf;
5.2 any firm, organisation or person that provides the company with products or services;
5.3 any payment system the company uses;
5.4 regulatory governmental authorities or ombudsmen, or other authorities, including taxes authorities, where the company has a duty to share information;
5.6 third parties to whom payments are made on behalf of employees;
5.7 financial institutions from whom payments are received on behalf of customers;
5.8 any other operator not specified; and
5.9 employees, contractors and temporary staff and agents.

6. CROSS BORDER TRANSFER OF PERSONAL INFORMATION

Personal information may be transmitted transborder to the company's suppliers in other countries, and personal information may be stored in data services hosted outside South Africa, which may not have adequate data protection laws. The company will endeavour to ensure that its dealers and suppliers have adequate protection of personal information and that the consent of the clients or customers are obtained at all times except where it is for the benefit of the customer and there is no reasonable possibility to obtain such consent.

7. CROSS BORDER FLOW OF PERSONAL INFORMATION

The POPIA Act provides that personal information may only be transferred out of the Republic of South Africa if:

7.1 the recipient country can offer such data and adequate level of protection, i.e. its data privacy laws must be substantially similar to that contained within the POPIA Act; or
7.2 the consumer consents to the transfer of their personal data; or
7.3 the transfer is necessary for the performance of a contractual obligation between the customers and the company; or
7.4 the transfer is necessary for the performance of a contractual obligation between the company and a third party, in the interest of the client or customer; or
7.5 the transfer is for the benefit of the customer and it is not reasonably possible to obtain consent from the customer who would in all likelihood provide such consent;
7.6 the company may retain personal information collected from their customers for the period in which there is an ongoing legitimate business to maintain such personal information or to comply with applicable, legal, tax or accounting requirements.

8. SECURITY SAFEGUARDS

8.1 The company shall ensure the integrity and confidentiality of all personal information in its possession by taking responsible steps to identify all reasonably foreseeable risks to

information security and to establish and maintain appropriate safeguards against such risks.

8.2 The company uses a range of physical, electronic and procedural safeguards to do so. The company updates these safeguards from time to time in order to address new and emerging security threats.

8.3 The company trains people on privacy matters as appropriate and seeks to limit access to personal information to those employees who need to know that information.

8.4 The company implements appropriate security measures to protect all personal information that is in the company's possession against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access.

8.5 Where there are reasonable grounds to believe that personal information in the company's possession has been accessed or required by any unauthorised person, the company will notify the relevant regulator and the customer, unless a public body responsible for detection, prevention or investigation of offences or the relevant regulator informs the company that notifying the customer would impede a criminal investigation.

9. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

The customer has a right to the following related to the personal information kept by the company:

9.1 enquire what personal information the company has on record;

9.2 request access to the personal information that is held by the company;

9.3 ask the company to update, correct or delete any out of date or incorrect personal information on record;

9.4 unsubscribe from any direct marketing communications that may be sent to the customers;

9.5 object to the processing of any personal information in the company's possession;

9.6 the prescribed form attached to this manual annexed as annexure "X" may be submitted to the company at any time for correction or deletion of customers' personal information on the company's system.

10. DIRECT MARKETING

All direct marketing communication shall contain the company and/or the company's details and an address or method for the customer to opt out of receiving further marketing communication.

10.1 Direct marketing – Direct marketing by electronic means to existing customers is only permitted if the customer's details were obtained in the context of a sale and service and for the purpose of marketing the same or similar product. The customer must be given the opportunity to opt out of receiving direct marketing on each occasion of their direct marketing;

10.2 Consent – the company may send electronic direct marketing communication to the customers who have consented to receiving it. The company may only approach the customer for consent once;

10.3 Record keeping – the company shall keep records of dates of consent, wording of the consent, who obtained the consent, proof of opportunity to opt out on each marketing contact and record of opt-outs.

11. DESTRUCTION OF DOCUMENTS

11.1 The documents may be destroyed. Personal information documents may be destroyed after the termination of the retention periods specified herein or as determined by the company from time to time.

11.2 Each Department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis.

11.3 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.

11.4 Original documents must be returned to the holder thereof, failing which, they should be retained by the company pending such return.

11.5 Deletion of electronic records must be done in consultation with the ID Department to ensure that the deletion information is incapable of being reconstructed and/or removed.

12. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period

Companies Act	• Any documents, accounts, books, writing, records or other info that a company is required to keep in terms of the Act; • Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; • Copies of reports presented at the annual general meeting of the company; • Copies of annual financial statements required by the Act; • Record of directors and past directors, after the director has retired from the company; • Written comms to holders of securities and minutes and resolutions of directors' meetings, audit committee and directors' committees.	**7 years**

	• Registration certificate; • Memorandum of Incorporation and alterations and amendments; • Rules; • Securities register and uncertified securities register; • Register of company secretary and auditors and • Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	**Indefinitely**
Consumer Protection Act	• Full names, physical address, postal address and contact details; • ID number and registration number; • Contact details of public officer in case of a justice person; • Service rendered; • Cost to be recovered from the consumer; • Frequency of accounting to the consumer; • Amounts, sums, values, charges, fees, remuneration specified in monetary terms; • Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions.	**3 years**

Financial Intelligence Centre Act	• Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; • If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; • If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; • The manner in which the identity of the persons referred to above was established; • The nature of that business relationship or transaction; • In the case of a transaction, the amount involved and the parties to that transaction; • All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; • The name of the person who obtained the identity of that person transaction on behalf of the accountable institution; • Any document or copy of a document obtained by the accountable institution.	**5 years**

Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees	**4 years**
	Section 20(2) documents: • Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; • Records of incidents reported at work.	**3 years**
	Asbestos Regulations 2001, Regulation 16(1): • Records of assessment and air monitoring, and the asbestos inventory; • Medical surveillance records Hazardous Biological agents Regulations 2001, Regulations 9(1) and (2): • Records of risk assessments and air monitoring; • Medical surveillance records Lead Regulations 2001, Regulation 10: • Records of assessments and air monitoring; • Medical surveillance records Noise-induced Hearing Loss Regulations 2003, Regulation 11: • All records of assessment and noise monitoring • All medical surveillance records, including the baseline audiogram of every employee	**40 years**
	Hazardous Chemical Substance Regulations 1995 Regulation 9: • Records of assessments and air monitoring; • Medical surveillance records	**30 years**

Basic Conditions of Employment Act	Section 29(4): • Written particulars of an employee after termination of employment; Section 31: -Employee's name and occupation; • Time worked by each employee; • Remuneration paid to each employee; • Date of birth of any employee under the age of 18 years	**3 years**
Employment Equity Act	• Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; • Section 21 report which is sent to the Director General	
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	
	An employee must retain prescribed details of any strike, lock-out or protest action involving its employees	**Indefinite**
Unemployment Insurance Act	Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed	**5 years**
Tax Administration Act	Section 29 documents which: • Enable a person to observe the requirements of the Act; • Are specifically required under a Tax Act by the Commissioner by the public notice; • Will enable SARS to be satisfied that the person has observed these requirements.	**5 years**

Income Tax Act	• Amount of remuneration paid or due by him to the employee; • The amount of employee's tax deducted or withheld from the remuneration paid or due; • The income tax reference number of that employee; • Any further prescribed information ; • Employer Reconciliation return.	**5 years**
Value Added Tax Act	• Where a vendor's basis of accounting is changed, the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; • Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; • Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; • Documentary proof substantiating the zero rating of supplies; • Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as descried in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	**5 years**