HUMAN RESOURCES **PROTECTION OF PERSONAL INFORMATION POLICY**	

POLICY NO	**:**	**HR27**
EDITION	**:**	**1**
EFFECTIVE DATE	**:**	**Immediate**
DRAFTER	**:**	**J. Visser**
COMPULSORY DISTRIBUTION:		**All personnel**

INDEX

PROTECTION OF PERSONAL INFORMATION POLICY

SECTION: Protection of Personal Information **Chapter HR27.1.**
SUBJECT: The Acts which Govern the Protection of Information in Context (1)

ACTS THAT GOVERN THE PROTECTION AND ACCESSING OF INFORMATION

1. The Protection of Personal Information Act No 4 of 2013 was signed into law 19 November 2013. Parts of the law became effective on 11 April 2014 whilst the rest were introduced gradually some years thereafter in 2020 and 2021.

2. Also referred to as the POPI Act or POPIA, this Act applies to any business which operates in South Africa or who have customers in the country. The Act broadly requires businesses to limit their use of personal data, get consent before using it, and it allows users to withdraw their consent at a later stage.

3. The Promotion of Access to Information Act, No. 2 of 2000 (PAIA) promotes transparency, accountability and good governance by empowering and educating the public to:

   3.1. Understand and exercise their rights,

   3.2. Understand the functions and operations of public bodies, and

   3.3. Effectively scrutinise and participate in decision-making by public bodies that affect their rights.

4. It is important to note that both these Acts must be read together as they supplement each other as far as the matter of protecting and dealing with personal information is concerned.

5. In order for the company to comply with POPIA it has to implement a Protection of Personal Information (POPI) programme which addresses matters such as the procedures and steps to be followed, and the documents and instruments to be used to ensure that the process of protecting personal information is executed in line with the legal requirements.

6. For the purposes of compliance and ease of reference, two separate policy documents address the above elements. This policy focusses on the requirements of the POPI Act and mainly on the limitations and requirements pertaining to the company's use of personal information, whereas the PAIA Policy and Procedure broadly deals with the matter of requesting, accessing and obtaining "informed" consent prior to accessing personal information.

PERSONAL INFORMATION POLICY

PURPOSE

1. DDP deals with and holds personal, customer and restricted information. The safeguarding thereof is important to help protect the interests and confidentiality of the company, its employees and its customers. As information security cannot be achieved by technical/technological means alone, it must be applied and enforced by people as well. This requires that every employee within the company understands what has to be done and how to do it in order to not place the company at risk by compromising the security of personal information.

INTRODUCTION

2. The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (POPIA).

3. POPIA aims to promote the protection of privacy through providing conditions which must be applied for the lawful processing of personal information of South Africans in a context-sensitive manner.

4. Through the provision of quality services and/or goods, the company is essentially involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

5. A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

6. Given the importance of privacy, the company is committed to effectively managing personal information in accordance with POPIA's provisions.

APPLICATION

7. This policy and its guiding principles apply to:

   7.1. the company's governing (executive) body.

   7.2. all branches, business units, divisions and other companies within the group.

   7.3. all employees and volunteers within the company.

   7.4. all contractors, suppliers, third parties and other persons acting on behalf of the company.

   7.5. any qualifying person that requires access to personal or company information.

8. The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the company's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

9. The legal duty to comply with POPIA's provisions is activated in any situation where there is:

   A **processing** of…..…
   personal information…….
   entered into a **record**…….
   by or for a **responsible person**……
   who is **domiciled** in South Africa.

10. POPIA does not apply in situations where the processing of personal information

10.1. is concluded in the course of purely personal or household activities, or

10.2. where the personal information has been de-identified.

PRINCIPLES

11. The company guarantees its commitment to protecting their client's privacy and ensuring their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

12. The principle as contained in Section 9 of the POPI Act states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive". This principle must be adhered to by all employees every time information is processed.

13. The company will inform its clients as to how their personal information is used, disclosed and destroyed.

UNDERTAKINGS

14. Prior to granting access to information or information systems, checks must be done to ensure that the individual requiring or requesting such access is suitable for access thereto. Therefore, the individual requesting the information must be cleared and granted permission to access such information and the individual must be authorised to deal with such information (need to know) in line with his/her work requirements and within their official capacity.

15. Users must be trained and equipped to work with information and to use systems securely and their access must be regularly reviewed to ensure it remains appropriate.

16. When a user's requirement for access to information or information systems end, access must be removed in a controlled manner. (i.e., when a user terminates their employment with the company, or changes their role so that access is no longer required).

17. Employees will be made aware of this policy and its requirements.

18. In order to obtain a copy of this policy the procedure as contained in the company's PAIA policy manual must be followed.

DEFINITIONS AND TERMINOLOGIES

19. The following meanings will apply:

19.1. 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.

19.2. Consent. Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

19.3. Data Subject. This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the company with services and/or products and/or other goods.

19.4. Direct Marketing. Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

19.4.1. Promoting or offering to supply, in the ordinary course of business, any services, products or goods to the data subject; or

19.4.2. Requesting the data subject to make a donation of any kind for any reason.

19.5. De-Identify. This means to delete any information that identifies a data subject or which can be used or manipulated by a reasonably foreseeable method to identify that data subject, or can be linked by a reasonably foreseeable method to other information, that identifies the data subject.

19.6. 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.

19.7. Governing Body. The Governing Body of the company will also mean Executive Board of Directors

19.8. Information Officer. The Information Officer is responsible for ensuring the company's compliance with POPIA. Where no Information Officer is appointed, the head of the company will be responsible for performing the Information Officer's duties. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA, prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

19.9. Operator. An 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. For example, a third-party service provider that has contracted with the company to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

19.10. Personal Information. Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

19.10.1. race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;

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

19.10.3. any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

19.10.4. the biometric information of the person;

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

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

19.10.7. the views or opinions of another individual about the person;

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

19.11. Processing. The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

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

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

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

19.12. Record. Means any recorded information, regardless of form or medium, including:

19.12.1. Writing on any material;

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

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

19.12.4. Book, map, plan, graph or drawing;

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

19.13. Re-Identify. In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

19.14. Responsible Party. The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the company is the responsible party.

19.15. Restriction. Means to withhold from circulation, use or publication of any personal information that forms part of a filing system but not to delete or destroy such information.

19.16. Special Personal Information. The Act, in section 26, classes some data as "special personal information", namely 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. This category also covers alleged criminal offenses and related court proceedings.

19.17. 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.

RATIONALE

20. The justification for this policy is to protect the company from the compliance risks associated with the protection of personal information which includes:

    20.1. Breaches of Confidentiality. For instance, the company could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.

    20.2. Failing to Offer a Choice. For instance, all data subjects should be free to choose how and for what purpose the company uses information relating to them.

    20.3. Reputational Damage. For instance, the company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the company.

COMPANY COMMITMENT TO PROTECTING THE PRIVACY OF DATA SUBJECTS

21. This policy demonstrates the company's commitment to protecting the privacy rights of data subjects in the following manner:

    21.1. Through stating the desired behaviour that is required and directing compliance with the provisions of POPIA and best practices.

    21.2. By cultivating a company culture that recognises privacy as a valuable human right.

    21.3. By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

    21.4. By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the company.

    21.5. By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the company and data subjects.

    21.6. By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

RIGHTS OF DATA SUBJECTS

22. Where applicable, the company will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

23. The company will ensure that it gives effect to the following rights:

    23.1. The Right to be Informed. The data subject has the right to be notified that his, her or its personal information is being collected by the company. The data subject also has the right to be notified in any situation where the company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

    23.2. The Right to Access Personal Information. The company recognises that a data subject has the right to establish whether the company holds personal information related to him, her or it including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under Annexure HR27.2.A.

23.3. The Right to have Personal Information Corrected or Deleted. The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the company is no longer authorised to retain the personal information.

23.4. The Right to Object to the Processing of Personal Information. The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, the company will give due consideration to the request and the requirements of POPIA. The company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

23.5. The Right to Object to Direct Marketing. The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

23.6. The Right to Not be Subjected to Automated Processing. Not to be subjected to a decision which is based solely on the basis of automated processing of his, her or its personal information intended to provide a profile of such person, thereby evaluating certain personal aspects in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, loan application etc. In terms of Section 71(1) certain circumstances do exist when this will not apply. These are, if the decision has been taken in connection with the conclusion or execution of a contract, and the request of the data subject in terms of the contract has been met; or appropriate measures have been taken to protect the data subject's legitimate interests; or is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

23.7. The Right to Complain to the Information Regulator. The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information. An example of a "POPI Complaint Form" can be found under Annexure HR27.2.B.

23.8. The Right to Take Legal Action. To institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

GENERAL GUIDING PRINCIPLES

24. All employees and persons acting on behalf of the company will at all times be subject to, and act in accordance with, the following guiding principles:

24.1. Accountability.

24.1.1. Failing to comply with POPIA could potentially damage the company's reputation or expose the company to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

24.1.2. The company will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the company will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

24.2. Processing Limitation.

24.2.1. The company will ensure that personal information under its control is processed:

24.2.1.1. in a fair, lawful and non-excessive manner, and

24.2.1.2. only with the informed consent of the data subject, and

24.2.1.3. only for a specifically defined purpose.

24.2.2. The company will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

24.2.3. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the company will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

24.2.4. The company will under no circumstances distribute or share personal information between separate legal entities, associated company's (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

24.2.5. Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the company's business and be provided with the reasons for doing so. An example of a "POPI Notice and Consent Form" can be found under Annexure HR27.2.C.

24.3. Purpose Specification.

24.3.1. All of the company's business units and operations must be informed by the principle of transparency.

24.3.2. The company will process personal information only for specific, explicitly defined and legitimate reasons.

24.3.3. The company will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

24.4. Further Processing Limitation.

24.4.1. Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

24.4.2. Therefore, where the company seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the company will first obtain additional consent from the data subject.

24.5. Information Quality.

24.5.1. The company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

24.5.2. The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the company will put into ensuring its accuracy.

24.5.3. Where personal information is collected or received from third parties, the company will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

24.6. Open Communication.

24.6.1. The company will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

24.6.2. The company will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

24.6.2.1. Enquire whether the company holds related personal information, or

24.6.2.2. Request access to related personal information, or

24.6.2.3. Request the company to update or correct related personal information, or

24.6.2.4. Lodge a complaint concerning the processing of personal information.

24.7. Security Safeguards.

24.7.1. The company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

24.7.2. Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

24.7.3. The company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the company's IT network.

24.7.4. The company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

24.7.5. All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the company is responsible.

24.7.6. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

24.7.7. The company's operators and third-party service providers will be required to enter into service level agreements with the company where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

24.7.8. An example of "Employee Consent and Confidentiality Clause" for inclusion in the company's employment contracts can be found under Annexure HR27.2.D.

24.7.9. An example of an "SLA Confidentiality Clause" for inclusion in the company's service level agreements can be found under Annexure HR27.2.E.

24.8. Data Subject Participation.

24.8.1. A data subject may request the correction or deletion of his, her or its personal information held by the company.

24.8.2. The company will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

24.8.3. Where applicable, the company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

INFORMATION OFFICERS

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

26. The company's Information Officer is responsible for ensuring compliance with POPIA.

27. There are no legal requirements under POPIA for a company to appoint an Information Officer. Appointing an Information Officer is however considered to be a good business practice, particularly within larger companies.

28. Where no Information Officer is appointed, the head of the company will assume the role of the Information Officer.

29. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

30. Once appointed, the company will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

31. An example of an "Information Officer Appointment Letter" can be found under Annexure HR27.2.F.

SPECIFIC DUTIES AND RESPONSIBILITIES

GOVERNING BODY

32. The company's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the company meets its legal obligations in terms of POPIA.

33. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

34. The governing body is responsible for ensuring that:

    34.1. The company appoints an Information Officer, and where necessary, a Deputy Information Officer.

    34.2. All persons responsible for the processing of personal information on behalf of the company:

        34.2.1. are appropriately trained and supervised to do so

        34.2.2. understand that they are contractually obligated to protect the personal information they come into contact with, and

        34.2.3. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

    34.3. Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

    34.4. The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the company collects, holds, uses, shares, discloses, destroys and processes personal information.

INFORMATION OFFICER

35. The company's Information Officer is responsible for:

    35.1. Taking steps to ensure the company's reasonable compliance with the provision of POPIA.

    35.2. Keeping the governing body updated about the company's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

    35.3. Continually analysing privacy regulations and aligning them with the company's personal information processing procedures. This will include reviewing the company's information protection procedures and related policies.

    35.4. Ensuring that POPI Audits are scheduled and conducted on a regular basis.

    35.5. Ensuring that the company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the company. For instance, maintaining a "contact us" facility on the company's website.

    35.6. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the company. This will include overseeing the amendment of the company's employment contracts and other service level agreements.

    35.7. Encouraging compliance with the conditions required for the lawful processing of personal information.

    35.8. Ensuring that employees and other persons acting on behalf of the company are fully aware of the risks associated with the processing of personal information and that they remain informed about the company's security controls.

35.9. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the company.

35.10. Addressing employees' POPIA related questions.

35.11. Addressing all POPIA related requests and complaints made by the company's data subjects.

35.12. Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

DEPUTY INFORMATION OFFICER

36. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

IT FUNCTION

37. As the company does not have a dedicated position for an IT Manager, the responsibilities relating to this type of function will be allocated to a manager who will be required to fulfil this function together with his or her primary function. This person will be responsible for:

37.1. Ensuring that the company's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.

37.2. Ensuring that all electronically held personal information is kept only on designated drives and servers and when uploaded only to approved cloud computing services.

37.3. Ensuring that servers containing personal information are sited in a secure location, away from the general office space.

37.4. Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.

37.5. Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.

37.6. Ensuring that personal information being transferred electronically is encrypted.

37.7. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.

37.8. Performing regular IT audits to ensure that the security of the company's hardware and software systems are functioning properly.

37.9. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.

37.10. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the company's behalf. For instance, cloud computing services.

MARKETING AND COMMUNICATION FUNCTION

38. As the company does not have a dedicated position for a Marketing and Communications Manager, the responsibilities relating to this type of position will be allocated to a manager who will be required to fulfil this function together with his or her primary function. This person will be responsible for:

    38.1. Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the company's website, including those attached to communications such as emails and electronic newsletters.

    38.2. Addressing any personal information protection queries from journalists or media outlets such as newspapers.

    38.3. Where necessary, working with persons acting on behalf of the company to ensure that any outsourced marketing initiatives comply with POPIA.

EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF THE COMPANY

39. This section must be read in conjunction with the security and confidentiality clause as contained in the employees' contract of employment as well as the Safety and Security Policy number HR6, with specific reference to Chapter HR6.3. paragraph 10.9. and in the case of persons acting on behalf of the company, the applicable Service Level Agreement.

40. Employees and other persons acting on behalf of the company will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

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

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

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

44. Employees and other persons acting on behalf of the company will only process personal information where:

    44.1. The data subject, or a competent person where the data subject is a child, consents to the processing; or

    44.2. The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or

    44.3. The processing complies with an obligation imposed by law on the responsible party; or

    44.4. The processing protects a legitimate interest of the data subject; or

    44.5. The processing is necessary for pursuing the legitimate interests of the company or of a third party to whom the information is supplied.

45. Furthermore, personal information will only be processed where the data subject:

    45.1. Clearly understands why and for what purpose his, her or its personal information is being collected; and

    45.2. Has granted the company with explicit written or verbally recorded consent to process his, her or its personal information.

46. Employees and other persons acting on behalf of the company will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

47. Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

48. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the company will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

49. Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

    49.1. the personal information has been made public, or

    49.2. where valid consent has been given to a third party, or

    49.3. the information is necessary for effective law enforcement.

50. Employees and other persons acting on behalf of the company will under no circumstances:

    50.1. Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.

    50.2. Save copies of all official information directly on the company server. This includes official information on private computers, laptops and/or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the company's central database or a dedicated server. Under no circumstances may any official information be stored on private computers or any other electronic devices.

    50.3. Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.

    50.4. Transfer personal information outside of South Africa without the expressed permission from the Information Officer.

51. Employees and other persons acting on behalf of the company are responsible for:

    51.1. Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.

    51.2. Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

51.3. Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The Manager tasked with IT responsibilities will assist employees and where required, other persons acting on behalf of the company, with the sending or sharing of personal information to or with authorised external persons.

51.4. Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

51.5. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

51.6. Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

51.7. Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

51.8. Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.

51.9. Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.

51.10. Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner and to ensure that record is kept of all deletions and disposals.

51.11. Undergoing POPI Awareness training from time to time.

52. Where an employee, or a person acting on behalf of the company, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer using the Occurrence Report Form Annexure HR6.3.A (attached to this policy for ease of use) as contained in the Safety and Security Policy, Number HR6.

<u>POPI AUDIT</u>

53. The company's Information Officer will schedule periodic POPI Audits.

54. The purpose of a POPI audit is to:

54.1. Identify the processes used to collect, record, store, disseminate and destroy personal information.
54.2. Determine the flow of personal information throughout the company. For instance, the company's various business units, divisions, branches and other associated companies.

54.3. Redefine the purpose for gathering and processing personal information.

54.4. Ensure that the processing parameters are still adequately limited.

54.5. Ensure that new data subjects are made aware of the processing of their personal information.

54.6. Re-establish the rationale for any further processing where information is received via a third party.

54.7. Verify the quality and security of personal information.

54.8. Monitor the extent of compliance with POPIA and this policy.

54.9. Monitor the effectiveness of internal controls established to manage the company's POPI related compliance risk.

55. In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the company's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

56. Information Officers will be permitted direct access to and have demonstrable/definite support from line managers and the company's governing body in performing their duties.

REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

57. Data subjects have the right to:

57.1. Request what personal information the company holds about them and why.

57.2. Request access to their personal information.

57.3. Be informed of the process that must be followed to keep their personal information up to date.

58. Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

59. Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the company's PAIA Policy.

60. The Information Officer will process all requests within a reasonable time.

POPI COMPLAINTS PROCEDURE

61. Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The company takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

61.1. POPI complaints must be submitted to the company in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form" (Annexure HR27.2.B).

61.2. Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.

61.3. The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

61.4. The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.

61.5. The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the company's data subjects.

61.6. Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the company's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

61.7. The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the company's Executive Board of Directors (governing body) within 7 working days of receipt of the complaint. In all instances, the company will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

61.8. The Information Officer's response to the data subject may comprise any of the following:

61.8.1. A suggested remedy for the complaint,

64.8.2. A dismissal of the complaint and the reasons as to why it was dismissed,

64.8.3. An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

61.9. Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to lodge a complaint with the Information Regulator.

61.10. The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

DISCIPLINARY ACTION

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

63. In the case of ignorance or minor negligence, the company will undertake to provide further awareness training to the employee.

64. Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

65. Examples of immediate actions that may be taken subsequent to an investigation include:

    65.1. A recommendation to commence with disciplinary action.

    65.2. A referral to appropriate law enforcement agencies for criminal investigation.

    65.3. Recovery of funds and assets in order to limit any prejudice or damages caused.

ANNEXURE HR27.2.A

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address:	

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

A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Request	
I request the company to:	
1. Inform me whether it holds any of my personal information	☐
2. Provide me with a record or description of my personal information	☐
3. Correct or update my personal information	☐
4. Destroy or delete a record of my personal information	☐

C. Instructions

D. Signature Page
Signature
Date

ANNEXURE HR27.2.B

POPI COMPLAINT FORM

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

Please submit your complaint to the Information Officer:	
Name	
Contact Number	
Email Address:	

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

The Information Regulator

Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria

Email: inforreg@justice.gov.za

Website: http://www.justice.gov.za/inforeg/index.html

A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature:	
Date	

ANNEXURE HR27.2.C

POPI NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details	
Name	
Contact Number	
Email Address:	

Purpose for Processing your Information

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches
- To issue, administer and manage your valuation
- To process valuations and to take the required action
- To notify you of new products or developments that may be of interest to you
- To confirm, verify and update your details
- To comply with any legal and regulatory requirements

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Consent to Disclose and Share your Information

We may need to share your information to provide advice, reports, valuations, analyses, products or services that you have requested.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I hereby authorise and consent to the company sharing my personal information with the following persons:
Name & Surname
Signature
Date

ANNEXURE HR27.2.D

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

1. "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

2. "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

3. The EMPLOYEE hereby undertakes to:
   3.1. comply with the requirements of the POPI Act,
   3.2. maintain the confidentiality of the Personal Information (PI) of the Company ("the Responsible Party")'' Data Subjects, (Customers, Clients, Suppliers, Sub-Contractors, Service Providers and EMPLOYEEs),
   3.3. notify the company's Information Officer/Deputy Information Officer immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person. Such notification should be done both verbally and in writing by the EMPLOYEE and the Occurrence Report Form, as contained in Policy Number HR27, Annexure HR27.2.G. must be completed by the EMPLOYEE for this purpose.

4. The EMPLOYER undertakes to process the PI of the EMPLOYEE only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the EMPLOYER's relevant policy available to the EMPLOYEE on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an EMPLOYER and within the framework of the employment relationship and as required by South African law.

5. The EMPLOYEE acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the EMPLOYER. The EMPLOYEE therefore irrevocably and unconditionally agrees:
   5.1. That the EMPLOYEE is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the EMPLOYER'S discharge of its obligations and to perform its functions as an EMPLOYER.
   5.2. That he/she consents and authorises the EMPLOYER to undertake the collection, processing and further processing of the EMPLOYEE'S PI by the EMPLOYER for the purposes of securing and further facilitating the EMPLOYEE'S employment with the EMPLOYER.
   5.3. Without derogating from the generality of the afore stated, the EMPLOYEE consents to the EMPLOYER'S collection and processing of PI pursuant to any of the EMPLOYER'S Internet, E-mail and Interception regulations as contained in the Electronic Communications Policy in place insofar as PI of the EMPLOYEE is contained in relevant electronic communications.
   5.4. To make available to the EMPLOYER all necessary PI required by the EMPLOYER for the purpose of securing and further facilitating the EMPLOYEE'S employment with the EMPLOYER.
   5.5. To absolve the EMPLOYER from any liability in terms of POPIA for failing to obtain the EMPLOYEE'S consent or to notify the EMPLOYEE of the reason for the processing of any of the EMPLOYEE'S PI.
   5.6. To the disclosure of his/her PI by the EMPLOYER to any third party, where the EMPLOYER has a legal or contractual duty to disclose such PI.

6. The EMPLOYEE further agrees to the disclosure of his/her PI for any reason enabling the EMPLOYER to carry out or to comply with any business obligation the EMPLOYER may have or to pursue a legitimate interest of the EMPLOYER in order for the EMPLOYER to perform its business on a day-to-day basis.

7. The EMPLOYEE authorises the EMPLOYER to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the EMPLOYER within the international community. The EMPLOYER undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

8. The EMPLOYEE acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other EMPLOYEE'S. The EMPLOYEE will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other EMPLOYEE'S.

9. The EMPLOYER reserves the right to intercept and/or monitor any direct or indirect communications systems on their work devices and telecommunication systems provided to the EMPLOYEE by the EMPLOYER to promote the EMPLOYER'S business objectives and which must be used for bona fide business purposes only.

10. To the extent that the EMPLOYEE is exposed to or insofar as PI of other EMPLOYEEs or third parties are disclosed to the EMPLOYEE, the EMPLOYEE hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or EMPLOYEE'S.

11. EMPLOYEE'S may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the company or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the EMPLOYEE or person to perform his or her duties on behalf of the EMPLOYER.

ANNEXURE HR27.2.E

SLA CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE HR27.2.F

INFORMATION OFFICER APPOINTMENT LETTER

I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the company's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the company's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the company's personal information processing procedures. This will include reviewing the company's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the company, to do so. For instance, maintaining a "contact us" facility on the company's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the company. This will include overseeing the amendment of the company's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the company are fully aware of the risks associated with the processing of personal information and that they remain informed about the company's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the company.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the company's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I hereby accept the appointment as Information Officer
Name & Surname
Signature
Date

ANNEXURE HR27.2.G

OCCURRENCE REPORT FORM

DATE OF OCCURRENCE _____ DATE OF REPORT_____

TIME OF OCCURRENCE ____ H ____ Requires immediate attention by manager: __ Yes __No

NAME OF PERSON REPORTING OCCURRENCE: _____

LOCATION OF OCCURRENCE: _____

BRIEF DESCRIPTION OF OCCURRENCE_____

_____

_____

_____

_____

IMMEDIATE ACTION TAKEN TO MITIGATE RISK (If any)

_____

_____

_____

_____
SIGNATURE OF REPORTING PERSON

ACTION TAKEN

CORRECTIVE ACTION TAKEN/IMPLEMENTED

_____

_____

_____

_____

_____
SIGNATURE OF INFORMATION OFFICER/DEPUTY INFORMATION OFFICER

NAME AND SURNAME: _____

DATE: : _____