Protection of Personal Information Policy

DOC NO: CAX-POL-031

Document Issued

2024/12/20

APPROVAL		
Morne Terblanche		20 December 2024
Name and Surname	Signature	Date

TABLE OF CONTENTS

CONTROL SHEET FOR AMENDMENTS

DATE	NATURE OF CHANGE	REVISION
13 May 2021	Initial Release	01
2 February 2023	Reviewed Policies	1.1
20 December 2024	Reviewed Policy, remove reference to HelpMe portal	1.2

1 INTRODUCTION

CyberAntix has a legal and social responsibility towards protecting personal information of any data subject. We have a duty of secrecy regarding provision or disclosure of personal information acquired from shareholders, board members, employees, contractors, customers or suppliers to an outside party without the intended reasons for use and without good reason.

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”).

PoPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Our company strongly recognizes the importance of appropriate safeguarding of such personal information held by us. Through the provision of quality goods and services, the Company is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

2 PURPOSE

a. The purpose of this policy is to incorporate the requirements of the POPI Act into the daily operations of the Company and to ensure that these requirements are documented and implemented in the business processes.
b. The objective of this policy is to ensure the constitutional right to privacy, with regards to:
    i. the safeguarding of personal information;
    ii. the regulation and processing of personal information;
    iii. the execution of the prescribed requirements for the legal processing of personal information; and
    iv. the protection of free flow of personal information.
c. The Company and its employees shall adhere to this policy concerning the management of all personal information received from, but not limited to natural persons, employees, clients, suppliers, agents, representatives and partners of the Company, to ensure compliance to this Act and the applicable regulations and rules relating to the protection of personal information is adhered to.

3 KEY DEFINITIONS AND ABBREVIATIONS

ABBREVIATION	DEFINITION
ICT	Information Communication Technology
IMC	Information Management Committee
PAIA	The Promotion of Access to Information Act No. 2 of 2000
PI	Personal Information
PoPIA	The Protection of Personal Information Act No. 4 of 2013 (in this Guideline the abbreviation is used interchangeably with the “Act”)

CAX	CyberAntix

ACRONYM OR WORD	DEFINITION
Biometrics	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.
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	The person to whom personal information relates. Data subjects within employment context includes applicants and former job applicants (successful or unsuccessful), former or current employees, temporary employment services staff, casual staff, staff on secondment and those on work experience placements. The personal information of all of these persons must be dealt with in accordance with POPI.
De-Identify	This means to delete any information that identifies a data subject, or which can be used by a reasonable foreseeable method to identify, or when linked to other information, that identifies the data subject.
Direct Marketing	To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of- a. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or b. Requesting the data subject to make a donation of any kind for any reason
Filing System	Any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
Information Officer	The Information Officer is responsible for ensuring the Company's compliance with PoPIA.
Operator	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.
Personal Information	Information relating to an identifiable, living, natural person, and where 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, well-being, 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 numbers, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d. The biometric information of the person; e. The personal opinions, views or preference of the person; f. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g. The views or opinions of another individual about the person; and h. The name of the person if it appears with another personal information relating to the person or if the disclosure of the name itself would reveal information about the person
Processing	Any operation or activity or any set of operations, whether 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
Record	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 other device in which one or more visual images are embodies 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

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.
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.; A full list of definitions can be viewed at Popia.co.za
SharePoint	SharePoint is a web-based collaborative platform that integrates with Microsoft Office. SharePoint is primarily a document management and storage system.

4 POLICY

4.1 POLICY APPLICATION

This policy and its guiding principles applies to:

- The Company's governing body;
- All branches, business units and divisions of the Company;
- The permanent or temporary employees and independent contractors of the Company;
- All contractors, suppliers and other persons acting on behalf of the Company;
- Any joint ventures, and/or other business organisations that are owned or controlled by the Company who receive or process personal information for, or on behalf of the Company;
- Personal information of external data subjects and data owners processed and/or stored by the Company, as well as the personal information of Company personnel.

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).

PoPIA does not apply in situations where the processing of personal information:

- Is concluded in the course of purely personal or household activities, or
- Where the personal information has been de-identified.

4.2 SCOPE

The contents of this policy is applicable to all employees of the Company and has been introduced in order to encourage the protection and confidentiality of all personal information that has been made available to the Company by employees or any client or supplier or any party who has disclosed any information of a private or business nature, for the sole intention of employment, business transactions, contracts or communication and will be deemed to be necessary for the records pertaining to the Company.

The information officer is the custodian of this policy, and responsible to ensure that this policy is incorporated and implemented in the various divisions of the Company, and that training is provided to all parties concerned regarding the contents of the Protection of Personal Information Act (PoPIA).

The Company will make employees aware of this policy by discussing it during induction sessions, monthly awareness training and by distributing it to the workforce by making it available on the Company's Document Management System through SharePoint.

However, it remains the duty and responsibility of all employees to make themselves aware of, and to familiarize themselves with, the content and application of this document.

4.3 CONDITIONS FOR PROCESSING PERSONAL INFORMATION

Processing and further processing of personal information is only lawful if it complies with the eight conditions for the processing of information specified in POPI. A data subject has the right to have his or her personal information processed in accordance with these conditions. All employees and persons acting on behalf of the Company will always be subject to, and act in accordance with, the following guiding principles:

4.3.1 Accountability

The responsibility for the protection and provision of access to information vests directly with the executive controlling body, board and senior executive management.

In order to safeguard this information, the Company established an appropriate information security management system. This provides for:

- the identification of the Company's information assets;
- a risk management methodology defining how the risk relating to the company's information assets is to be determined;
- the implementation of controls to mitigate the identified risks;
- appropriate policies, processes and standards governing the use of information within the Company; and
- mechanisms for the continuous and ongoing review of the company's information management and security.

The company appoints an information officer who will be responsible for overseeing compliance with the provisions of POPI. The appointed and registered information officer will conduct a personal information impact assessment to ensure that the Company has adequate measures and protocols in place to comply with the conditions of lawful processing of personal information.

The Company remains responsible for the processing of information regardless of it having transferred or communicated that personal information to a third party (defined as an "Operator"), to process the personal information.

4.3.2 Processing Limitation

The Company will ensure that personal information under its control is processed:

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

- Only with the informed consent of the data subject; and
- For a specifically defined purpose.

All data subjects must be informed of the reasons the Company is collecting his/her personal information and obtain written consent prior to processing personal information.

Consent forms can be found as specified in the Reference section.

4.3.3 Purpose Specification

The Company will process personal information only for specific, explicitly defined and legitimate reasons. The Company will inform the data subject of these reasons prior to collecting or recording the data subject's personal information.

Where there are no statutory and legal requirements prescribing retention periods, the company may only retain records of personal information for as long as it is necessary to achieve the specific purpose for which the information was collected.

4.3.4 Further Processing Limitations

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

The Company may use personal information if it is compatible with or in accordance with the purpose for which it was collected in the first place. Where this secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the data subject.

4.3.5 Information Quality

The Company will take reasonable steps to ensure that all personal information collected is complete, accurate, not misleading and updated where necessary.

Special care is required where information is collected from a source other than the employee personally. The Company will then take reasonable steps to verify directly with the data subject that the information is correct.

4.3.6 Open Communication

The Company must take reasonable and practical steps to ensure that the data subject is aware of the information collected and the source of the information. This includes the name and address of the data subject's company, the purpose for which it is collected, whether the data subject is obliged to supply the information and what law if any, prescribes the disclosure of the information to the Company/employer.

The Company will ensure that it establishes a "contact" capability via its website or through an internal helpdesk portal, for data subjects who want to:

- Enquire whether the Company holds related personal information, or
- Request access to related personal information, or
- Request the Company to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

4.3.7 Security Safeguards

The Company will 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 loss of or damage to or unauthorised destruction, unlawful access to or processing of personal information.

The reasonable measures to protect the personal information include identification of possible security risks, establish and maintain safeguards against the risks, verify the safeguards from time to time and update those measures. Virus programmes, back-ups, secure storage, access control and off-site storage are all measures to consider. The measures must comply with generally accepted information security practices.

Any employee or third party can only process information when authorized to do so by the Company and must treat the personal information as confidential.

All employees processing personal information will be required to sign employment contracts containing confidentiality clauses to reduce the risk of unauthorized disclosure of personal information for which the Company is responsible. The Company must also ensure that an operator not domiciled in the Republic, adheres to the laws governing the processing of personal information.

Where a breach of personal information is suspected, the employee must immediately notify the Company. If such a breach is confirmed, the Company has the responsibility to report the breach to the Regulator and inform the data subjects whose personal data were compromised to take protective measures against the potential consequences of the compromise.

A contractual agreement will be drawn up between the Company and third-party service providers, which contains the requirements for the protection of personal data for which the Company is responsible. Both parties must agree to the lawful processing of any personal information.

4.3.8 Data Subject Participation

A data subject may request:

- To confirm, free of charge, whether the Company holds personal information about him/her;
- For a reasonable fee, a description of the personal data held; and
- The correction or deletion of his/ her personal information held by the Company.

The Company will ensure that it establishes a “contact” capability via its website or through an internal helpdesk portal for data subjects who want to request the correction of deletion of their personal information.

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

4.4 ROLES & RESPONSIBILITIES

4.4.1 Information/Deputy Officers

CAX has appointed an Information Officer and Deputies in terms of the Act. The Information Officer will be duly registered with the Information Regulator as is required by the applicable legislation after its establishment and will report to the Board of Directors of the Company.

The Company will also designate where necessary, an appropriate number of Deputy Information Officers. The Deputy Information Officers will also be duly registered with the Information Regulator after establishment as is required, reporting directly to the Information Officer of the Company and will in conjunction with the Information Officer and any other designated individuals constitute the official Information Management Committee (hereafter also referred to as the "IMC") of the Company, which will be communicated as such to all Company employees and other relevant parties.

Responsibilities are as follows:

- Ensure a compliance framework is developed, implemented, monitored and maintained;
- Ensure a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- Develop a manual which is, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA;
- Processes are developed together with adequate systems to process requests for information or access thereto;
- 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;
- 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 regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator;
- 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 Officer 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.

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

4.4.2 IT Manager

The IT Manager is responsible for definition, implementation, and technical maintenance of security devices and technologies that constitute the Organization's ICT networks and resources and the Information Security Management System.

The person in this Role is responsible, among other things, for:

- Definition and implementation of technical safety controls in the Company;
- Participation in the risk analysis process with the support of technical experts;
- Supervision of access rights to the Company's resources;
- Responding to threats and security incidents in the Company;
- Support and implementation of components constituting a part of operation continuity plans in the Company including backup and disaster recovery solutions;
- Raising awareness of users in technological areas;
- Maintenance of ICT infrastructure and resources based on the Operational Activity Process;
- Ensuring that the necessary software solutions are provided to employees to ensure personal information transferred electronically is encrypted;
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software. These servers must be sited in a secure location;
- Performing scheduled Vulnerability Assessments to ensure that the security of the Company's hardware and software systems is not compromised;
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons;
- 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.

4.4.3 Marketing and Communication Manager

The Company's Marketing and Communication Manager is responsible for:

- 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;
- Addressing any personal information protection queries from journalists or media outlets such as newspapers; and
- Where necessary, working with persons acting on behalf of the Company to ensure that any outsourced marketing initiatives comply with PoPIA.

4.4.4 Employees and Other Persons Acting on Behalf of the Company

During the performance of duties, employees and other persons acting on behalf of the Company (Data Processors), could have access to the personal information of certain clients, suppliers and other employees. They are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Data Processors 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.

Data Processors 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.

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

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- 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
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the information is supplied.

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

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the Company with explicit written or verbally recorded consent to process his/her personal information.

Employees and other persons acting on behalf of the organization 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.

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.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form.

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

- The personal information has been made public, or
- Where valid consent has been given to a third party, or
- The information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the organization will under no circumstances:

- 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;
- Save copies of personal information directly to their own private computers, laptops 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;
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure unless it is encrypted. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer;
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the Company are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy;
- Ensuring that personal information is held in as few places as is necessary. No unnecessary addition records, filing systems and data sets should therefore be created;
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager 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;
- 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;
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks;
- 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;
- 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;
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- 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;
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming as 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;
- 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;
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the organization, becomes aware or suspicious of any security breach such as the unauthorized 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.

4.5 RIGHTS OF DATA SUBJECTS

All data subjects including employees, customers and suppliers are made aware of their rights as data subjects. This is achieved through the inclusion of Data Protection clauses within contracts

and/or the acknowledgement of Consent for Use of Personal Information Agreements provided to these Data Subjects.

The rights of correction and deletion apply only to personal information that is:

- Inaccurate
- Irrelevant
- Excessive
- Out of date
- Incomplete
- Misleading
- Obtained unlawfully

The Company will ensure that it gives effect to the following six rights.

As prescribed by the Act and included in the Company's PAIA Manual, customers and employees can request access, corrections, destruction of information by using the prescribed forms as specified in the Reference section.

4.5.1 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.

4.5.2 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 including the right to request access to that personal information.

There are grounds on which the Company must or may refuse access to a record (in certain instances, this may be mandatory, in others it may be discretionary):

- Protection of the privacy of a third party who is a natural person;
- Protection of certain confidential information of a third party;
- Protection of commercial information of third party in terms of an agreement;
- Protection of the safety of individuals, and the protection of property;
- Protection of records used in legal proceedings;
- National Security

4.5.3 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 organization is no longer authorized to retain the personal information. The Company however can retain the records when it:

- Is required or authorised by law;

- Reasonably requires the record for lawful purposes related to its functions or activities;
- Is required by a contract between the parties thereto;
- The data subject has consented to the retention of the record.

4.5.4 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 organization 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.

4.5.5 The right to object to direct marketing

The data subject has the right to object to the processing of his/her personal information for purpose of direct marketing by means of unsolicited electronic communication.

4.5.6 The right not to be subject to decisions based on Automated Processing of Personal Information

The data subject has the right not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his/her personal information intended to provide a profile of such person.

4.5.7 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.

4.6 POPI AUDIT

The Company's Information Officer will schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information;
- Determine the flow of personal information throughout the Company. For instance, the Company's various business units, divisions, branches and other associated company's;
- Redefine the purpose for gathering and processing personal information;
- Ensure that the processing parameters are still adequately limited;
- Ensure that new data subjects are made aware of the processing of their personal information;
- Re-establish the rationale for any further processing where information is received via a third party;
- Verify the quality and security of personal information;
- Monitor the extend of compliance with PoPIA and this policy;

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

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

Information Officers or Deputy Information Officers will be permitted direct access to and have demonstrable support from line managers and the Company's governing body in performing their duties.

4.7 ACCOUNTABILITY AND DISCIPLINARY ACTION

Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or non-compliance to the Company's policy prescriptions, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of the Company.

Where the Information Management Committee believes that the conduct may constitute a violation of any applicable law, rule, or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

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

The contractual agreements of external third party contractors to the Company will be subject to immediate suspension or termination in the sole discretion of the senior management of the Company, pending investigation and recommendations of the Information Management Committee of the Company.

5 REFERENCES

Document No	Document Name
CAX-FRM-032	Request For Information, Access, Corrections, Destruction Of Personal Records (Employees)
CAX-MAN-001	PAIA Manual
J752	PAIA Request for Access to Record Form C (External Data Subjects)
Form 1	Objection to the Processing of Personal Information
Form 2	Request for Correction or Deletion of Personal Information
Form 4	Obtain Data Subject Consent
CAX-FRM-030	Employee Personal Information Privacy Notice

Document No	Document Name
https://popia.co.za/act/	POPI Act
https://www.michalsons.com/	Michalsons Attorneys' website
LSSA (Law Society of South Africa) Guidelines	Protection of Personal Information for South African Law Firms
Information Regulator	Draft Guidelines on the Registration of Information Officers
https://serr.co.za	POPI Act- Obtaining Consent
https://www.tech4law.co.za	Processing Limitations
https://www.popiact-compliance.co.za/	Data Subject Rights