BOTHAVILLE APTEEK (EDMS)BPK

REGISTRATION NUMBER 2004/025819/07

POPIA POLICY

Title	Bothaville Apteek POPIA Policy
Custodian	Mr. Rudi Scheepers
Prepared by	Linde Attorneys
Location	Bothaville Apteek Website & Physical Address
Effective date	1 October 2021
Website	www.bothavilleapteek.co.za

PREAMBLE

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 principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, Bothaville Apteek is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

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.

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

The Policy is made available on Bothaville Apteek website www.bothavilleapteek.co.za and by request from Bothaville Apteek's physical address in President Avenue, Bothaville.

GLOSSARY

Definitions, Abbreviations and Acronyms

TERM	DEFINITION
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.
Child	means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

Competent Person	means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Confidential Information	any information, including Personal Information, in any format or material embodiment which is by its nature confidential and includes medical information, financial information, know-how, trade secrets, employee training programs and/or plans, processes, formulae, hypertext documents or language, programmes, algorithms, machinery, designs, drawings, plans, research, products, financial results and projections, business plans, ideas, account numbers software source code, inventions, business, financial and marketing objectives or strategies, technical specifications and data in whatever form, proprietary intellectual property and the like and includes the fact and extent of the owner's interest in same; client lists or prospective client lists and client details, including names, cell phone numbers and banking details; descriptions of corporate structure, shareholdings, franchise and licensing arrangements; any written information which is labelled "confidential" or "proprietary" before it is disclosed, belonging to or relating to the party disclosing such information ("Disclosing Party") which information is communicated to or otherwise acquired by the other Party ("Receiving Party"), during the course of the Parties' interactions, discussions and negotiations with one another, whether such information is formally designated as confidential or not.
Consent	any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data message	includes a data message as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002); "form(s)" as referred to in these Regulations, means a form referred to in the annexures to these Regulations or any form which is substantially similar to that form.
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 Bothaville Apteek with products or other goods.
De-identify	This means to delete any information that identifies a data subject or which can be used by a reasonably 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: ✦ Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or ✦ Requesting the data subject to make a donation of any kind for any reason.
Disclosing Party	Means the party disclosing personal information.
ECTA	Electronic Communications and Transactions Act
Electronic communication	any text, voice, sound or image message sent over an electronic communications network, which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Electronic Communications system	all systems used by Bothaville Apteek that enable electronic communications, including (without limitation) the Internet, voice mail, electronic mail and facsimiles.

Employee	Means a part- or fulltime employee of Bothaville Apteek
FICA	Financial Intelligence Centre Act No. 38 OF 2001, as amended
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.
Information matching programme	the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject
Information officer	The Information Officer is responsible for ensuring Bothaville Apteek's compliance with PoPIA. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIAA prior to performing his or her duties.
IO	Information Officer
Natural person	An individual that establishes a business relationship or enters into a single transaction with an accountable institution and includes a trust, partnership or sole proprietor.
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 Bothaville Apteek up 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.
PAIA	Promotion of Access to Information Act
Person	Means a natural or a juristic person
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: ✦ 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; ✦ 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
PI	Personal Information

POPIAA	Protection of Personal Information Act, 2013
Private body	means— (a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; (b) a partnership which carries or has carried on any trade, business or profession; (c) or any former or existing juristic person, but excludes a public body
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: ✦ the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; ✦ dissemination by means of transmission, distribution or making available in any other form; or ✦ merging, linking, as well as any restriction, degradation, erasure or destruction of information.
Public body	means— (a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when— (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation
Receiving party	the person receiving personal information, for whatever purpose.
Record	any recorded information, regardless of form or medium, including: ✦ Writing on any material; ✦ Medical prescription; ✦ 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; ✦ Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; ✦ Book, map, plan, graph or drawing; ✦ 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.
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 Person	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, Bothaville Apteek is the responsible party.
Restriction	Means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information

Special Personal Information	Means personal information concerning: (a) The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings
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.

1. POLICY PURPOSE

1.1 Statement and purpose

1.1.1 The value of information as an asset to Bothaville Apteek cannot be underestimated. The ever-increasing dependence of Bothaville Apteek on information systems creates a unique vulnerability for our business, requiring the introduction of business rules to provide clear and definitive instructions to assist Bothaville Apteek in securing its information.

1.1.2 The term "information security" refers to the management of the integrity, availability and confidentiality of the lifeblood of our organisation, which includes business trade secrets, contractual relationships, intellectual property, financial and operational systems, client and transaction details and information published to the public.

1.1.3 A breach in information security may compromise Bothaville Apteek's ability to provide goods or services, be the cause of losses in revenue through fines or penalties and fraud, destruction of proprietary or confidential data, lead to breaches of business contracts, trade secrets and privacy or damage our reputation with our stakeholders.

1.1.4 Information security is regarded as a critical part of Bothaville Apteek risk management programmes. This policy provides a framework for the safeguarding of our organisational information, compliance with relevant legislation and to serve as reference documents for internal quality control processes.

1.1.6 The responsibility to preserve Bothaville Apteek's information security requires the co-operation of every employee. This policy has accordingly been written with the following goals in mind:

1.1.6.1 To describe staff obligations to satisfying the requirements of the Protection of Personal Information Act (PoPIA);
1.1.6.2 to establish business rules to ensure the integrity, availability and confidentiality of all Bothaville Apteek information;
1.1.6.3 to educate employees about their obligations for the protection of all Bothaville Apteek information; and
1.1.6.4 to be read in conjunction with any other policy as well as the PAIA Manual.

1.2 Status and application of policy

This policy applies to Bothaville Apteek and should also be conveyed and applied to all contractors, suppliers and other persons acting on behalf of Bothaville Apteek.

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**.

POPIA does not apply in situations where the processing of personal information is conducted in the course of purely personal or household activities, or where the personal information has been de-identified.

All employees are bound to this document as part of the Bothaville Apteek standard terms and conditions of employment.

Where non-employees, such as contractors, are permitted access to Bothaville Apteeks' information systems, they shall likewise contractually be required to adhere to the terms of this policy.

1.3 Updates and amendments

Updates to this policy and related information shall from time to time be published on the Bothaville Apteek website.

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least annually.

1.4 Further Information

Further information about this document can be obtained from the Information Officer, as defined below.

2 PRIVACY

2.1 Statutory appointments

The Information Officer of Bothaville Apteek is RUDOLPH HENDRIK SCHEEPERS whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and POPIA.

This policy has been put in place by Bothaville Apteek and training on this policy and the POPIA Act will be conducted by Bothaville Apteek.

2.2 Audit process

Compliance with this policy shall be monitored by the Information Officer on an informal basis from time to time.

2.3 Collection of evidence

In the event that an employee suspects that a breach of this policy may have occurred on an information system (whether relating to Bothaville Apteek or client information), no further action is permitted in respect of such information system until such time as the IO has authorised same.

2.4 Information Classification

Information Classification is the process of assigning value to information in order to organize it according to its risk to loss or harm from disclosure.

The classification process is set out in the Data Classification Policy, whilst the handling thereof is set out in the Data Handling Policy.

3. LAWFUL PROCESSING CONDITIONS

The following obligations apply to all Bothaville Apteek staff when collecting, processing or destroying Personal Information. Should any staff member require clarity on any aspect of these requirements, their queries may be directed at either the Information Officer.

3.1 Accountability

The Information Officer will ensure that the conditions and all the measures set out in the Act are complied with at the time of determining the purpose and means of the processing.

Accordingly, the Information Officer will ensure the following:
- Bothaville Apteek will identify and appoint resources as required across the organization to fulfil the requirements wherever personal information is processed
- The relevant stakeholders are adequately trained to fulfil their obligations
- Awareness programs are provided to ensure that all staff are aware of the Act and its implications for daily operations
- Privacy risk is determined through assessments, and reported via the existing risk management channels
- The existence, location and use of personal information is recorded and monitored
- Data subject requests are recorded and addressed wherever they occur, in line with the PAIA Manual
- Related legislation is integrated into privacy management, including specific consideration of retention periods and monitoring
- Bothaville Apteek registers with the Regulator and remains current with published regulations as these occur
- Third-party contracts adequately account for compliance with the Act

3.2 Processing Limitation

Personal information may **only** be processed in a fair and lawful manner and only with the consent of the data subject, unless specifically prescribed by any law.

Staff must ensure the following:

- **Personal information must be obtained directly from the Data Subject. The data subject must be referred to the Bothaville Apteek Notice PRIOR to providing personal information.**
- **The Data Subject must be aware that you have gathered his/her information and consented to the information being used.**
- **The Data Subject must have consented to information being shared and used by you, if the personal information has been gathered from a third party.**
- **The amount of information being gathered may not be excessive.**
- **Consent to process client information is obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship**
- **Should any third parties request access to personal information processed by Bothaville Apteek, this may only be provided with the approval of the Bothaville Apteek Information**

Officer. Conversely, when a third party shares personal information they are processing, Bothaville Apteek must ensure that this is with the approval of an authorised individual within their organization.

3.3 Purpose Specification

Personal information may only be processed for specific, explicitly defined and legitimate reasons.

The staff member must ensure the following:

- **The specific, explicit and lawful purpose for which the personal information is being collected must be documented and adhered to.**
- **The Data Subject must be aware of the purpose for which the data has been collected.**
- **All personal information collected must correspond to legitimate reasons for collecting.**
  - **Personal information may only be retained for the time periods specified in law.**
  - **Keep track of when personal information must be destroyed.**
  - **Document the process that will be used to destroy Personal Information, in a manner that prevents its reconstruction, after you are no longer authorized to retain such record.**

3.4 Further processing limitation

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

The staff member must ensure the following:

- **The intended reuse of personal information must be in accordance and compatible with the purpose for which it was collected.**
- **The Data Subject must be aware of the continued use of their personal information.**

3.5 Information quality

The responsible party must take reasonably steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.

- **Ensure that personal information is reliable and accurate at all times.**
- **Data Subjects may update their information or withdraw consent by contacting Bothaville Apteek.**

3.6 Openness

The data subject whose information you are collecting must be aware that you are collecting such personal information and for what purpose the information will be used.

The Operator must ensure the following:

- **Proof of consent for collecting and using personal information from the Data Subject is extremely important. Consent must be explicit, and evidence of consent must be retained. Silence does not equal consent.**
- **The Data Subject must be informed of the purpose for which the information is being gathered at the time the information is being gathered or as soon as practically possible after collection.**
- **Inform the Data Subject who the responsible party is.**
- **Inform the Data Subjects of their right to lodge a complaint with the Information Regulator.**

- **Advise the Data Subject of his/her rights to access his/her information and to object to the processing of said information.**

3.7 Security Safeguards

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

The Responsible Person must determine and ensure:

- **Identify procedures to identify any foreseeable internal and external risks to personal information.**
- **Identify processes to prevent personal information from falling into unauthorized hands.**
- **Determine which employees are permitted access to personal information and what information they are permitted to access.**
- **Identify processes to alert you when personal information is accessed or modified without authorization.**
- **Determine processes to identify the source of a data breach and the procedure to follow to neutralize such breach.**
- **Continually update safeguards in response to new risks or deficiencies in previously implemented safeguards.**
- **Prevent and/or address the reoccurrence of a data breach.**
- **Ensure Non-disclosure agreements, alternatively data protection addendums are in place when sharing personal information with an external operator.**
- **Inform the Data Subject that their personal information has been compromised.**
- **Inform the Information Regulator of any security breach.**

3.8 Data subject participation

Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them.

Staff must ensure that Data Subjects are advised as follows:

- **The Data Subject's rights regarding access to information being held by Bothaville Apteek.**
- **The Data Subject's right to correct personal information that Bothaville Apteek holds or withdraw consent to use such information.**

4. SAFEGUARDING PI

Bothaville Apteek 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.

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

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

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

Employment contracts contain contractual terms for the use and storage of employee information. Confidentiality clauses are or will be included to reduce the risk of unauthorised disclosures of personal information for which Bothaville Apteek is responsible.
The following procedures are in place in order to protect personal information:

- Every employee, current or new, employed will be subjected to compliance with this Policy;
- Bothaville Apteek archived client information is stored on site which is also governed by POPIA, access is limited to these areas to authorized personal.
- All electronic files or data are backed up;

Documents may also be stored off-site, in storage facilities approved by Bothaville Apteek.

5. DESTRUCTION

Documents may be destroyed after the termination of the retention period specified in law. Should there be a need to retain information beyond this point for statistical or trend analysis, the personal information must be de-identified prior to this occurring.

6. CLEAN DESK POLICY

6.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

6.2 Computer workstations must be locked when workspace is unoccupied.

6.3 Computer workstations must be shut completely down at the end of the workday.

6.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

6.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

6.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

6.7 Laptops must be either locked with a locking cable or locked away in a drawer.

6.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

6.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

6.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

6.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

6.12 Lock away portable computing devices such as laptops and tablets.

6.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer All printers and fax machines should be cleared of papers as

soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

6.14 Business Premises Access:

6.14.1 Physical access to facilities containing sensitive information shall be restricted in a manner directed by the IO.

7. TRANSFER OF PI

7.1 Internally

PI may only be transferred internally amongst Bothaville Apteek employee or third parties if:

- There is a legitimate purpose, for example, between pharmacists in the interest of the customer; or
- The Data Subject has specifically consented to the transfer; or
- The third party has signed a non-disclosure agreement to protect personal data and/or the Data Subject has consented thereto.

8. ACCEPTABLE USE OF ASSETS

8.1 Company property

Electronic communication systems and all messages generated on or handled by an employee is considered to be the property of Bothaville Apteek.

8.2 No expectation of privacy

Bothaville Apteek may automatically monitor the use of the electronic communication systems and may be required to review the contents of stored or transmitted data in the course of their duties.

8.3 Encryption of electronic communications and devices

8.3.1 Employees should note that most electronic communications are by default not secure.

8.3.2 In certain instances, this policy prescribes the use of encryption technologies.

8.3.3 Electronic communications may only be encrypted utilising technologies approved by the IO and further subject to any conditions imposed in respect thereof in terms of procedures.

8.4 Acceptable and unacceptable use

8.4.1 Employees must comply with the Bothaville Apteek's Acceptable Use Policy in place from time to time.

8.4.2 Employees are to comply with all policies related and to be implemented simultaneously with this Policy.

9. DIRECT MARKETING

There is no restriction on direct marketing by electronic communication to existing customers, provided that the customer is afforded the opportunity of opting out of further communications with the responsible party.

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

10. VIOLATION

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

Bothaville Apteek 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, Bothaville Apteek 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.

BOTHAVILLE APTEEK (EDMS)BPK

REGISTRATION NUMBER 2004/025819/07

ACCEPTABLE USAGE POLICY

Title	Bothaville Apteek Acceptable Usage Policy
Custodian	Mr. Rudi Scheepers
Prepared by	Linde Attorneys
Location	Bothaville Apteek Website & Physical Address
Effective date	1 October 2021
Website	www.bothavilleapteek.co.za

1.0 ACCEPTABLE USAGE

Overview

All users, including but not limited to employees, contractors and third-party personnel shall judiciously use Bothaville Apteek information/information assets in order to reduce the threats to Bothaville Apteek's information systems, applications, equipment and network devices. This document provides guidelines for the acceptable use of Bothaville Apteek information/information assets, information systems, applications, equipment, and network devices.

1.1 SECURING PROPRIETARY INFORMATION

The following guidelines shall be adhered to in order to secure proprietary information at Bothaville Apteek:

a. All users shall comply with Bothaville Apteek's POPIA Policy.
b. Users shall have no proprietary rights or interest in any idea, invention, design, technical or business innovation, computer program and related documentation, or work product (hereinafter referred to as "intellectual property") developed by the user for Bothaville Apteek.
c. Users shall acknowledge and sign confidentiality/non- disclosure agreement which states that all intellectual property developed or used during employment is a property of Bothaville Apteek.

d. Any unauthorised distribution of proprietary or classified information including but not limited to corporate strategies, competitor sensitive information, trade secrets, specifications, customer lists, customer's medical information shall be prohibited and shall result in disciplinary action against the user.
e. On termination of employment/contract, user shall promptly return all Bothaville Apteek assets including but not limited to manuals, disks, documents, papers, and other materials.
f. On termination of employment/contract, the information assets under user's possession or under the user's control that may contain sensitive information shall be returned to Bothaville Apteek.

1.2 E-MAIL USAGE

E-mail is a widely used medium for exchange of information between two or more individuals and for business communication; hence the usage of the e-mail shall be governed by Bothaville Apteek. The following sections provide guidelines to ensure that emails are used as an efficient mode of business communication and that the email services are not misused by the users.

ACCEPTABLE USE OF E-MAIL

The guidelines related to acceptable use of e-mail at Bothaville Apteek have been defined in the following section:

a. All messages generated by the e-mail system shall be considered the property of Bothaville Apteek.
b. Bothaville Apteek reserves the right to monitor email use to ensure compliance with Bothaville Apteek's Acceptable Usage Guidelines.
c. The e-mail system shall be used for business purposes only. However, the personal use of the e-mail systems shall be approved by the Information Officer and may be allowed as long as it does not damage the information and/or reputation of Bothaville Apteek.
d. The users shall not open attachments received from unknown senders, which may contain malware such as viruses, worms, or Trojans.

PROHIBITIVE USE OF E-MAIL

The guidelines related to prohibitive use of e-mail at Bothaville Apteek are defined in the following section:

a. Using e-mails for charitable fundraising campaigns not sponsored by Bothaville Apteek, political advocacy efforts, private business activities or personal amusement and entertainment.
b. Creating or distributing any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin.
c. Forwarding or sending messages that have racial or sexual slur, political or religious solicitations.
d. Transmitting any material that potentially contains viruses, Trojan horses, e-mail bombs or any other harmful or malicious program.
e. Defaming, abusing, harassing, stalking, threatening or violating any legal and privacy laws.
f. Business related e-mails shall not be sent from a private e-mail account.
g. Sharing e-mail account login information with other users.

1.3 INTERNET USAGE

This section provides general guidelines for use of internet for either official or personal purpose:

a. Access to the Internet from corporate intranets shall be controlled with primary focus to reduce risk of virus infection and hacking.
b. Access to the Internet shall be granted for business-related purposes only. The access shall be restricted to the authorised personnel only.
c. Bothaville Apteek shall reserve the right to record and monitor internet usage. Any inappropriate use of the internet may result in a disciplinary action.
d. Downloads from the Internet shall be screened for viruses prior to use/installation on Bothaville Apteek's information systems.
e. The downloading of non-approved software onto Bothaville Apteek's systems without the prior written consent from the Information Officer prohibited.
f. In case the information from the Internet is used for Bothaville Apteek business decisions, the integrity and the source of the information shall be verified. Additionally, care shall be taken not to violate any copyright laws when using information obtained from the Internet.
g. Personal use of internet shall be permitted so long as it does not adversely affect Bothaville Apteek's activities or reputation.

h. Web content filtering shall be enabled to restrict accessing inappropriate sites. Inappropriate websites shall be blocked from users. The websites related to following shall be restricted:
    i. Sites known to be a cyber security threat
    ii. Unapproved tunnels and related protocols / proxy networks
    iii. Pornographic sites
    iv. Gambling sites
    v. Terrorism groups
    vi. Social media
    vii. Religious Fundamentalist groups
    viii. Hatred groups.

i. Employees shall not attempt to probe other information systems, applications, equipment and network devices for security weaknesses.

1.4 CHAT ROOMS, SOCIAL NETWORKING AND INSTANT MESSAGING

The following section provides guidelines for the use of chat rooms, social networking and instant messaging, especially when dealing with business information:

a. Subscriptions to chat rooms, instant messaging services and or social networking sites shall be done in a responsible manner.
b. All users, unless authorised, shall not represent Bothaville Apteek or express Bothaville Apteek's views on a matter in chat rooms, instant messaging services or on social networking sites unless authorized to do so by the Information Officer.
c. Employees should explicitly mention that no views/opinions expressed by them in chat rooms, instant messaging services and on social networking sites represent the views/opinions of Bothaville Apteek.
d. Downloading and transferring of files from social networking sites to and from Bothaville Apteek workstations shall be prohibited.
e. Creating or distributing any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin is prohibited.

1.5 REMOTE ACCESS USAGE

The following section provides guidelines regarding remote access usage:

a. The remote access shall be provided to the users only on approval from the relevant Information Officer.
b. Bothaville Apteek reserves the right to refuse to extend remote access privileges to any user and may refuse or terminate remote access arrangement at any time.
c. Special care shall be taken while using mobile computing devices including but not limited to laptops, notebooks, tablet PCs, PDAs and mobile phones to ensure that the organisational information stored thereon is not compromised.
d. The accessibility of equipment and software provided for remotely accessing Bothaville Apteek network shall be limited to authorised personnel and for business related purposes.

1.6 PRINTERS USAGE

The following section provides guidelines related to acceptable use of printers at Bothaville Apteek:

a. Access to Bothaville Apteek letterheads for printing shall be restricted to authorised personnel only.
b. Access to colour printers shall be restricted to the authorised personnel only.
c. Printing of personal items such as photos and personal e-books shall be prohibited.
d. Printed hard copies of sensitive information shall be protected and destroyed after use as per the guidelines below:
    i. Shredding shall be the primary means of the disposal of paper media containing sensitive information.
    ii. All paper media identified for disposal shall be kept in designated, locked boxes for shredding or otherwise shall be kept secure until shredded.
    iii. The disposal of sensitive information shall be performed by authorised personnel only and a proof of destruction shall be obtained and recorded.

1.7 SOFTWARE USAGE

The following section provides guidelines related to acceptable use of software at Bothaville Apteek:

a. Bothaville Apteek provides users workstations or other mobile computing devices. All software required to maintain and to keep track of the workstations and mobile computing devices are installed on these devices and shall not be tampered with.
b. The access to tools/systems used for tracking IT related assets shall be restricted to authorised personnel.

c. Bothaville Apteek shall not support any non-standard system configurations and shall reserve the right to remove such systems from the network should they pose a security risk to Bothaville Apteek.

d. Installation of any unauthorised or unlicensed software on the workstations shall be prohibited.

e. Interruption of any automated installation of patches, software or service packs on workstation shall be prohibited.

f. All software shall be procured through the Information Officer exclusively.

g. The retrieval of executable files/source codes of the software procured, including freeware or shareware shall be strictly prohibited, unless the license agreement allows for the retrieval.

h. Commercial software purchased by Bothaville Apteek shall be authorised for Bothaville Apteek use only and shall be utilised in accordance with contractual agreements and copyright laws.

i. Making copies of copyright protected software and related documentation for personal use shall be prohibited, unless specifically authorised within the license agreement.

j. Bothaville Apteek reserves the right to remove all unauthorised software and the personnel using such software shall be subject to disciplinary action.

BOTHAVILLE APTEEK (EDMS)BPK

REGISTRATION NUMBER 2004/025819/07

DATA CLASSIFICATION POLICY

Title	Bothaville Apteek Data Classification Policy
Custodian	Mr. Rudi Scheepers
Prepared by	Linde Attorneys
Location	Bothaville Apteek Website & Physical Address
Effective date	1 October 2021
Website	www.bothavilleapteek.co.za

PREAMBLE

INFORMATION CLASSIFICATION

Three classification levels are identified and referred to as Level 1, Level 2, and Level 3. Although all the enumerated information values require some level of protection, particular data values are considered more sensitive and correspondingly tighter controls are required for these values.

All Bothaville Apteek information should be reviewed on a periodic basis and classified according to its use, sensitivity and importance to Bothaville Apteek and in compliance with relevant laws. The level of security required will depend in part on the effect that unauthorized access or disclosure of those data values would have on Bothaville Apteek operations, functions, image or reputation, assets, or the privacy of individual members of the Bothaville Apteek.

Each level will have a defined risk/sensitivity category indicating the potential harmful impact to Bothaville Apteek if the integrity of that resource is compromised:

- **High** - An unauthorized disclosure, compromise or destruction would result in severe damage to Bothaville Apteek or employees. Violation of legislation, regulations, or other legal obligations, financial loss, damage to Bothaville Apteek's reputation, and possible legal action could occur.
- **Moderate** - An unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on Bothaville Apteek or employees. Financial loss, damage to Bothaville Apteek's reputation, and possible legal action could occur.
- **Low** - Knowledge of this information does not expose Bothaville Apteek to financial loss or jeopardize the security of Bothaville Apteek's information assets.

Data Owner shall mean ownership vests in the management of Bothaville Apteek where the information is **created**, or that it is the **primary user** of the information. Bothaville Apteek retains actual legal ownership of information assets.

Custodian shall mean an employee designated by the Data Owner to be responsible for maintaining the safeguards established by the Data Owner.

User shall mean an employee authorised by the Data Owner to access information and use of the safeguards established by the Data Owner.

. . . table continues on next page

CLASSIFICATION LEVEL 1: CONFIDENTIAL

Confidential information is maintained by Bothaville Apteek that is prohibited from disclosure under certain relevant laws or classified as confidential by Bothaville Apteek. Confidential information is information whose unauthorized disclosure, compromise or destruction would result in severe damage to Bothaville Apteek or employees. Financial loss, damage to Bothaville Apteek's reputation, and possible legal action could occur. Level 1 information is intended solely for use by Bothaville Apteek employees. Statutes, regulation, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of Bothaville Apteek is governed by specific standards and controls designed to protect the information.

Risk/Sensitivity: High

Examples of Level 1 Information Include:

Personally Identifiable Information (PII)	Financial Information	Health Information	Law Enforcement Information
• Passwords or login credentials that grant access to level 1 and level 2 data • PINs (Personal Identification Numbers) • Birth date combined with last four digits of SSN and name • Driver's license number, state identification card number, and other forms of national or international identification (such as passports, visas, etc.) in combination with name • Identity number (**both complete and last 4 digits)** and name • Biometric information (e.g.: fingerprint, voice recording, palm print, iris scan, DNA) • Email addresses/username with password or security question responses • Electronic or digitized signatures • Private key (digital certificate)	• Credit card numbers with cardholder name • Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account • Tax ID with name	• Health insurance information • Medical records related to an individual customer of Bothaville Apteek • Psychological Counselling records related to an individual customer of Bothaville Apteek	• Law enforcement personnel records • Criminal background check results • Law enforcement records related to an individual • Vulnerability/security related to Bothaville Apteek law enforcement operations

CLASSIFICATION LEVEL 2: INTERNAL USE ONLY

Internal Use Only is information which must be protected due to proprietary or privacy considerations. Although possibly not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to Bothaville Apteek's reputation, violate an individual's privacy rights or legal action could occur.

Level 2 information is intended for Bothaville Apteek employees, contractors, and vendors covered by a non-disclosure agreement with a business need-to-know.

Risk/Sensitivity: Moderate

Examples of Level 2 Information Include:

<table>
<tr>
<th>Employee Information</th>
<th>Identity validation keys</th>
<th>Facilities Information</th>
</tr>
<tr>
<td rowspan="4">

Home or mailing address
Birthplace (City, Country)
Employee identification
Employee net salary
Employment history
Personal telephone numbers
Personal email address
Parents and other family members' names
Emergency contact names and telephone numbers
Payment history
Employee evaluations
Pre-employment background investigations
Race and ethnicity
Gender
Marital status
Personal characteristics (e.g., hobbies)
Physical description
Photograph (taken for identification purposes)

</td>
<td>

Birth date (full: mm-dd-yy)
Birth date (partial: mm-dd only)

</td>
<td>

Construction drawings of existing buildings
Maps of utility systems
Other detailed drawings of sensitive facilities

</td>
</tr>
<tr>
<th>Bothaville Apteek Donee Information</th>
<th>Legal Information</th>
</tr>
<tr>
<td>

Name
Home or mailing address
Personal telephone numbers
Personal email address
Donation

</td>
<td>

Attorney-client communications
Legal investigations conducted by Bothaville Apteek
Settlements and claims against Bothaville Apteek
Accident reports and investigations

</td>
</tr>
<tr>
<th>Bothaville Apteek Research</th>
<th>Purchasing and Accounts Payable Information</th>
</tr>
<tr>
<td>

Trade secrets or intellectual property such as research activities
Information covered by a specific non-disclosure agreement

</td>
<td>

Sealed bids prior to award
Identifiable information (purchase order) of the supplier/company

</td>
</tr>
</table>

	Technical Security Information	Other Information
	Vulnerability/security information related to a business or computer information system	• Location of critical or protected assets • Licensed software

CLASSIFICATION LEVEL 3: PUBLICLY AVAILABLE

Publicly Available is explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both employed and contracted (e.g., an employee's work email addresses), or not specifically classified elsewhere in the protected information classification standard. Knowledge of this information does not expose Bothaville Apteek to financial loss or jeopardize the security of Bothaville Apteek's assets. Publicly Available information may be subject to appropriate business review, facilities' procedures, employee's procedures, or third-party procedures to mitigate potential risks of inappropriate disclosure.

Risk/Sensitivity: Low Risk

Examples of Level 3 Information Include:

Employee Information	Financial Information	Third Party (Supplier) Information (Directory Information)
• Employee title • Company corporate email address • Employee work location and telephone number • Employing department • Name (first, middle, last) (except when associated with protected information) • Corporate Email Signature	• Limited Financial information • Purchase order information	• Name • Product or services Field • Registration dates as supplier • Full or Part-time status • Business telephone number • E-mail address

IMPORTANT NOTICE: PRESUMED CONSENT IF NO SIGNED FORM IS RETURNED

If we fail to receive a signed version of this form from you within 14 days succeeding the date hereof, we will accept such failure to be an acknowledgement of your consent we endeavour to seek herein.

BOTHAVILLE APTEEK (EDMS)BPK

REGISTRATION NUMBER 2004/025819/07

TEL NO: 056-515-2391
FAX NO: 056 515 4722
CELL NO: 072 455 5770

PO BOX 1495
BOTHAVILLE
9660
E-MAIL: bothaville@pro-pharm.co.za
Direkteure: Rudi Scheepers, Jo Scheepers, Linda Botha

ADRES:
PRESIDENT STREET 38
BOTHAVILLE
9660

Vat nr: 4960216820

THE PROTECTION OF PERSONAL INFORMATION ACT

CUSTOMER / CLIENT / VENDOR CONSENT NOTICE

Privacy is paramount

This Notice explains how we obtain, use and disclose your personal information, in accordance with the requirements of the Protection of Personal Information Act No 4 of 2013 ("**Act**").

We are committed to protecting your privacy and to ensure that your personal information is collected and used properly, lawfully and transparently.

Why?

We collect and process your personal information mainly to:

- Vendors / Service Providers / Insurers / Company Representatives:
  Registration / Purchase Orders / Payments / Trade referencing / Sharing information with Customers and Clients in order to render pharmaceutical and related retail services and products

- Customers / Clients:
  Medical and Health history / Registration of accounts / Background or credit checks / Invoices / Statements / Sharing of information with medical practitioners (if required) Vendors and / or Service Providers in order to render pharmaceutical and related retail services and products

We will use your personal information only for the purposes for which it was collected and agreed with you. In addition, where necessary your information may be retained for legal or research purposes.

What?

For this purpose, we will collect:

IMPORTANT NOTICE: PRESUMED CONSENT IF NO SIGNED FORM IS RETURNED

If we fail to receive a signed version of this form from you within 14 days succeeding the date hereof, we will accept such failure to be an acknowledgement of your consent we endeavour to seek herein.

Names, Identity Numbers, Registration Numbers, Trading names, Addresses, Vat nr's, Telephone Numbers, Fax Numbers, E-mail addresses, Bank details, Trade references, Marital status, Financial Information, Medical and Health History

We collect information directly from you where you provide us with your personal details.

Disclosure of information

We may disclose your personal information to our service providers / medical practitioners / customers / client / suppliers / vendors / insurers / company representatives who are involved in the delivery of products or services.

We may also disclose your information where we have a duty or a right to disclose in terms of law or industry codes, where we believe it is necessary to protect our rights or to our auditors, legal advisors, etc.

Storage and retention and destruction of information

We will store your personal information electronically in a centralised data base, which, for operational reasons, will be accessible to all within our company on a need to know and business basis, save that where appropriate, some of your personal information may be retained in hard copy.

We will ensure that your personal information which you provide to us will be held and/or stored securely.

Once your personal information is no longer required due to the fact that the purpose for which the personal information was held has come to an end and has expired, such personal information will be safely and securely archived for such periods as may be required by any law applicable in South Africa.

Thereafter we will ensure that such personal information is permanently destroyed.

Your Rights: Access to information

You have the right to request a copy of the personal information we hold about you. To do this, simply contact Mr. Rudi Scheepers, the intended Information Officer.

You have the right to ask us to update, correct or delete your personal information.

How to contact us

If you have any queries about this notice, you need further information about our privacy practices, if you wish to withdraw consent, exercise preferences or access or correct your personal information, please contact us.

Declaration and informed Consent

I, the signatory hereby acknowledge that I have read the terms and conditions reflected above, that I fully understand the meaning and effect thereof, that all personal information supplied to Bothaville Apteek (Pty) Ltd is accurate, up-to-date, not misleading and that it is complete in all respects, to immediately advise Bothaville Apteek (Pty) Ltd of any changes to the personal information should any of these details change, to give Bothaville Apteek (Pty) Ltd permission to process the personal

IMPORTANT NOTICE: PRESUMED CONSENT IF NO SIGNED FORM IS RETURNED

If we fail to receive a signed version of this form from you within 14 days succeeding the date hereof, we will accept such failure to be an acknowledgement of your consent we endeavour to seek herein.

information, as provided above, and acknowledge that I understand the purposes for which it is required and for which it will be used.

Signed at _____ on this _____day of _____ 2021.

_____

Company/Customer/Vendor/Supplier Name

_____ _____

(Print name in block letters) **Signature**

If on behalf of a Company/Trust or CC

BOTHAVILLE APTEEK (EDMS)BPK

REGISTRATION NUMBER 2004/025819/07

PRIVACY AND SECURITY NOTICE

Your right to privacy and security is very important to us. Bothaville Apteek (we, us, our) treat personal information as private and confidential.

How and why we collect personal information

- We collect personal information for the purposes set out in this notice or otherwise communicated to you.
- We collect personal information directly from you when you purchase our products or services or on receipt of a prescription from a healthcare practitioner.
- We may collect from and share your personal information with selected third parties to ensure we meet our responsibilities as a registered pharmacy.
- We collect personal information from and about you for the following purposes, but not limited to:
    - Assess your individual requirements accurately
    - Deliver effective and personalised services to you that comply with applicable regulations.
    - To identify potential markets and trends, evaluate and improve our business (this includes improving existing and developing new products and services)
    - Tell you about services and products available within the pharmacy
    - Constantly improve our offerings to suit your unique needs
    - To verify and protect your identity
    - Conduct credit checks, where applicable
    - Regulatory reporting
    - Comply with relevant regulatory requirements, including monitoring and analysing your account for credit, fraud, compliance and other risk-related purposes as required by law.
    - As otherwise allowed by law

Without your personal information, we may not be able to provide or continue to provide you with the products or services that you need.

What personal information do we collect?

We collect and process different attributes of your personal information at specific points of our business processes, to fulfil a legislative mandate or for internal business purposes. Please see below a non-exhaustive list of personal information categories that we collect and process.

- Identifying number (employee number; company registration numbers, ID number),
- Email-addresses, physical address, telephone number
- Names, surname, marital status, nationality, age, physical health status, mental health status, well-being, disability status, language, date of birth. Some of the information may be more prevalent in our employment processes than in the core business divisions.
- Information on your race, ethnic or social origin, criminal recordings/proceedings.
- Education, medical, financial, employment information

Storage and retention of personal information

We store personal information as required by law and take all relevant security safeguards to ensure the protection of the information.

The law defines how long we keep all types of records, including any personal information we process. Personal information is retained and destroyed as required or authorised by law.

Our use of technology to follow your use of our website

We collect and examine information about visits to this website. We use this information to find out which areas of the website people visit most. This helps us to add more value to our services. This information is gathered in such a way that we do not get personal information about any individual or their online behaviour on other websites.

Cookies

We may use cookie technology on some parts of our website. A cookie is small pieces of text that are saved on your Internet browser when you use our website. The cookie is sent back to our computer each time you visit our website. Cookies make it easier for us to give you a better experience online. You can stop your browser from accepting cookies, but if you do, some parts of our website or online services may not work. We recommend that you allow cookies.

Marketing by post, email or text messages

If you give us permission, we may use your personal or other information to tell you about products, services and special offers from us or other companies that may interest you. We will do this by post, email or text message (SMS and WhatsApp). If you later decide that you do not want us to do this, please contact us and we will stop doing so.

Third parties

We ask other organisations to provide support services to us. When we do this, they have to agree to our privacy policies if they need access to any personal information to carry out their services.

Our website may contain links to or from other websites. We try to link only to websites that also have high standards and respect for privacy, but we are not responsible for their security and privacy practices or their content. We recommend that you always read the privacy and security notices on these websites.

When we may reveal personal information without consent

We will not reveal personal information to anyone outside our business or certain of our service providers without your permission, unless:

- we must do so by law or in terms of a court order
- it is in the public interest
- we need to do so to protect our rights
- there is a legitimate purpose for the sharing
- we reasonably determine it to be in your best interest

Our security practices

- We are committed and obliged to implement all reasonable controls to safeguard access to your personal information.
- Where third parties are required to process your personal information in relation to the purposes set out in this notice and for other legal requirements, we ensure that they are contractually bound to apply the appropriate security practices.

Your right to access information

- You have the right to request access to the personal information we process about you. You may exercise this right by following the Promotion of Access to Information (PAIA) manual, available on the website.

- If you have any questions regarding this please let us know on **bothaville@pro-pharm.co.za**

Personal use of emails and notice about checking on emails

Our communication and information systems are for business use. However, we realise that our employees occasionally use our systems for personal use. Personal use includes sending or receiving personal emails within or outside Bothaville Apteek. We do not accept responsibility for the contents of personal emails sent by our employees using our systems. Please note that we may intercept, check on and delete any communications created, stored, sent, or received using our systems, according to any law that applies.

Right to change this privacy and security notice

We may always change this privacy and security notice. We will put all changes on our website. The latest version of our privacy and security notice will replace all earlier versions of it, unless it says differently.

Email us on **bothaville@pro-pharm.co.za** if you have any questions about this privacy and security notice.

Promotion of Access to Information Act

The Promotion of Access to Information Act (PAIA) was passed in order to give effect to the constitutional right of access to information held by a public or private body for the exercise or protection of any right.

Bothaville Apteek is a private body as defined in the Act. Bothaville Apteek is bound by this Act and shall process any request made in terms thereof.

Right of access to information

A requester must be given access to any information record of Bothaville Apteek if all the following requirements are met:

- The record is required for the exercise or protection of any right of the individual.
- The requester meets the procedural requirements of the act relating to a request for access to an information record.
- The request falls outside any of the grounds of refusal contemplated in the act.

Request procedure

The following procedure is applicable to requests for access to information in terms of the Act:

- The requester must complete in full the prescribed request form and send that to the Information Officer
- Where required to do so by the Information Officer, the requester must deposit a prescribed fee to ensure that processing takes place (The requester will be notified where the Information Officer requires a deposit)
- The completed request form and proof of deposit must be sent to:

  Particulars of Bothaville Apteek
  Information Officer
  38 President Street
  Bothaville
  9660
  E-mail: bothaville@pro-pharm.co.za

- Upon receipt of the request form and proof of deposit, Bothaville Apteek will:
  - Assess the request form to ensure completeness
  - Confirm receipt of the request fee
  - Process the request if it meets the procedural requirements of the act
  - Notify a third party where applicable
  - Decide whether to grant or deny the request
  - Let the requester know of the decision
  - Notify the requester about the payable access fee if the request is granted
  - Repay the request fee to the requester if the request is refused
  - Release the requested information record to the requester upon confirmation of receipt of the payable access fee