Umfolozi Sugar Mill (Pty) Ltd
Private Bag X12, Mtubatuba, 3935, South Africa
Tel: (035) 550 7700 Fax (035) 550 1145

Revision: 3 October 2022

USM PAIA AND POPI MANUAL

This manual was prepared in accordance with Section 51 of the Promotion of Access to Information Act, 2000 (PAIA) and to address requirements of the Protection of Personal Information Act, 2013 (POPIA).

This manual applies to the Umfolozi Sugar Mill (Pty) Ltd, Registration Number: 2008/012011/07 ("USM")

Registered Office Address: Corner Mill Road and Club Lane, Riverview, 3930

1 CONTENTS

2 USM CONTACT DETAILS

2.1 NATURE OF THE BUSINESS

2.1.1 USM is a manufacturer of high quality VHP brown sugar.

Company Name:	Umfolozi Sugar Mill (Pty) Ltd (USM)
Physical Address:	Corner of Mill Road and Club Lane Riverview, 3930 South Africa
Telephone Number:	+27 35 550 7700
Website:	https://www.umfolozisugarmill.co.za

2.2 CONTACT PERSONS

2.2.1 Requests pursuant to the provisions of PAIA and POPIA should be directed as follows:

CEO:	Adrian Wynne
Email:	Awynne@usm.co.za
Information Officer:	Riaan Oberholzer
Email:	Roberholzer@usm.co.za

2.2.2 The Information Officer has delegated powers to Deputy Information Officers in terms of PAIA and POPIA.

3 INTRODUCTION

3.1 THE PROMOTION OF ACCESS TO INFORMATION ACT (PAIA)

3.1.1 The Promotion of Access to Information Act No. 2 of 2000, (PAIA) came into operation in November 2001. Section 51 of this Act requires that USM as a private body compile a manual giving information to the public regarding the procedure to be followed in requesting information from USM for the purpose exercising or protecting rights. On request, the private body or government is obliged to release such information unless the PAIA expressly states that the records containing such information may or must not be released.

3.2 THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

3.2.1 The Protection of Personal Information Act, 2013 (POPIA) is intended to help protect Data Subjects from security breaches, theft, and discrimination through eight conditions for lawful processing of Personal Information:

1. Accountability
2. Processing limitation
3. Purpose specification
4. Further processing limitation
5. Information quality

6. Openness
7. Security safeguards
8. Data subject participation

3.2.2 The POPIA gives Data Subjects the right to, in a prescribed manner, request a Responsible Party to correct or delete Personal Information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or destroy or delete a record of Personal Information about the Data Subject that the Responsible Party is nolonger authorised to retain access and / or request the correction of any Personal Information held about them that may be inaccurate, misleading or outdated.

3.3 CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA

3.3.1 Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy. The right to privacy includes the right to protection against the unlawful collection, retention, dissemination and use of personal information.

3.4 SOUTH AFRICAN HUMAN RIGHTS COMMISSION GUIDE

3.4.1 A guide to the PAIA (as contemplated under section 10 of the PAIA) is available from the South African Human Rights Commission. The guide contains such information as may reasonably be required by a person who wishes to exercise any right contemplated in the PAIA.

3.4.2 Any enquiries regarding the PAIA guide and its contents should be directed to:

The South African Human Rights Commission
PAIA Unit (the Research and Documentation Department)
Postal address: Private Bag 2700, Houghton, 2041
Telephone: +27 11 484-8300
Fax: +27 11 484-7146
Website: https://www.sahrc.org.za
E-mail: PAIA@sahrc.org.za

3.5 USM POSITION

3.5.1 USM endorses the South African Human Rights Commission Guide and the constitutional right to protection against unlawful collection, retention, dissemination and use of personal information. Consequently, USM also endorse spirit of PAIA and POPIA and believes that this Manual will assist requesters in exercising their rights.

4 PAIA - PROMOTION OF ACCESS TO INFORMATION

4.1 RECORDS AUTOMATICALLY AVAILABLE - PAIA 51(1)(C)

4.1.1 In terms of Section 52 of PAIA no known notice has been gazetted for automatic access to legislated records.

4.1.2 All documentation and information that is available on the USM website is volunteered to be automatically available.

4.2 LEGISLATIVE RECORDS HELD BY USM - PAIA 51(1)(D)

4.2.1 Where applicable to its operations, USM retains records and documents in terms of the legislation below. Access to such related information may be restricted in terms of legislation, regulations, contractual

agreement or otherwise and if permitted shall be made available for inspection by interested parties in terms of the requirements and conditions of PAIA.

1. Auditing Professions Act, No 26 of 2005;
2. Basic Conditions of Employment Act, No 75 of 1997;
3. Broad- Based Black Economic Empowerment Act, No 75 of 1997;
4. Business Act, No 71 of 1991;
5. Companies Act, No 71 of 2008;
6. Compensation for Occupational Injuries & Diseases Act, 130 of 1993;
7. Competition Act, No.71 of 2008;
8. Constitution of the Republic of South Africa 2008;
9. Copyright Act, No 98 of 1978;
10. Customs & Excise Act, 91 of 1964;
11. Electronic Communications Act, No 36 of 2005;
12. Electronic Communications and Transactions Act, No 25 of 2002;
13. Employment Equity Act, No 55 of 1998;
14. Financial Intelligence Centre Act, No 38 of 2001;
15. Identification Act, No. 68 of 1997;
16. Income Tax Act, No 58 of 1962;
17. Intellectual Property Laws Amendment Act, No 38 of 1997;
18. National Environmental Management Act 107 of 1998;
19. National Environment Management: Air Quality Act 39 of 2004;
20. National Environmental Management: Waste Act 59 of 2008;
21. National Water Act 36 of 1998;
22. Labour Relations Act, No 66 of 1995;
23. Long Term Insurance Act, No 52 of 1998;
24. Occupational Health & Safety Act, No 85 of 1993;
25. Pension Funds Act, No 24 of 1956;
26. Prescription Act, No 68 of 1969;
27. Prevention of Organised Crime Act, No 121 of 1998;
28. Promotion of Access to Information Act, No 2 of 2000;
29. Protection of Personal Information Act, No. 4 of 2013;
30. Revenue Laws Second Amendment Act. No 61 of 2008;
31. Skills Development Levies Act No. 9 of 1999;
32. Short-term Insurance Act No. 53 of 1998;
33. Sugar Act No. 9 of 1978;
34. Unemployment Insurance Contributions Act 4 of 2002;
35. Unemployment Insurance Act No. 30 of 1966;
36. Value Added Tax Act 89 of 1991.

4.2.2 USM has used its best endeavours to supply a list of applicable legislation, it is possible that this list may be incomplete and USM shall update the list when an omission comes to USM's attention.

4.3 GENERAL RECORDS HELD BY USM - PAIA 51(1)(E)

4.3.1 The list below depicts broad non-exhaustive list of information records that USM keeps in terms of applicable laws. Access to such related information may be restricted in terms of legislation, regulations, contractual agreement or otherwise and if permitted shall be made available for inspection by interested parties in terms of the requirements and conditions of PAIA.

4.3.2 Companies Act Records

1. Company Incorporation
2. Names of Directors

3. Minutes of Board Meetings
4. Records relating to the appointment of directors / auditor / secretary / public officer and other officers

4.3.3 Financial Records

5. Financial Statements
6. Documents relating to taxation of the company
7. Accounting records
8. Fixed and moveable asset records

4.3.4 Agreements or Contract Records

9. Standard Agreements
10. Contracts concluded with Companies
11. Contracts concluded with Customers
12. Third Party Contracts (such as Service Level Agreements etc.)
13. Suppliers Contracts

4.3.5 Company Policies and procedures

14. Safety, Health, Environment and Quality
15. Internal relating to employees and the company
16. External relating to clients and other third parties

4.3.6 Legal and Regulatory

17. Licenses or Authorities

4.3.7 Supplier Information

18. Supplier Details
19. Contact details of individuals within Suppliers
20. Communications with Suppliers

4.3.8 Employees

21. List of Employees
22. Personal Information of Employees
23. Employee Contracts of Employment
24. Leave Records

4.3.9 Customer Information

25. Customer Details
26. Contact details of individuals within Customers
27. Communications with Customers

4.3.10 Systems, Solutions, and Information Technology

28. Intellectual property pertaining to solutions and products developed.
29. Usage of solutions and products

4.4 FEES

4.4.1 A personal requester is a requester who is seeking access to a record containing Personal Information about the requester.

4.4.2 A requester, other than a personal requester, is entitled to request access to information pertaining to such juristic person.

4.4.3 There are two types of fees: (1) a request fee (standard fee) and (2) an access fee (calculated by considering reproduction costs, search and preparation time and cost, as well as postal / courier costs where applicable). When a request is received by the Information Officer, the Information Officer shall by notice require the requester, other than a personal requester, to pay the prescribed request fee, before further processing of the request can take place.

4.4.4 If a search for the information is necessary and the preparation and disclosure of the information for disclosure, requires more time than prescribed in the regulations for this purpose, the Information Officer shall notify the requester to pay as a deposit if the request is granted.

4.4.5 The Information Officer shall withhold information until the requester has paid the fee or fees indicated. A requester whose request for access to information has been granted, must pay an access fee reproduction, for search, preparation, and for any time in excess of the prescribed hours to prepare the information for disclosure including making arrangements to make it available in the request form.

4.4.6 If a deposit has been paid in respect of a request for access, which is refused, then the Information Officer shall repay the deposit to the requester.

4.4.7 Fees can be scrutinised in ANNEXURE 1.

5 POPIA - PROTECTION OF PERSONAL INFORMATION

5.1 PROCESSING PERSONAL INFORMATION AND ITS PURPOSE

5.1.1 The minimum conditions for lawful processing of Personal Information by a Responsible Party are presented below and may not be derogated from unless specific exclusions apply as outlined in the POPIA:

1. Accountability - the Responsible Party has an obligation to ensure that there is compliance with the POPIA in respect of the Processing of Personal Information.
2. Processing limitation - Personal Information must be collected directly from a Data Subject to the extent applicable; must only be processed with the consent of the Data Subject and must only be used for the purposes for which it was obtained.
3. Purpose specification - Personal Information must only be processed for the specific purpose for which it was obtained and must not be retained for any longer than it is needed to achieve such purpose.
4. Further processing limitation - further processing of Personal Information must be compatible with the initial purpose for which the information was collected.
5. Information quality - the Responsible Party must ensure that Personal Information held is accurate and updated regularly and that the integrity of the information is maintained by appropriate security measures.
6. Openness - there must be transparency between the Data Subject and the Responsible Party.
7. Security safeguards - a Responsible Party must take reasonable steps to ensure that adequate safeguards are in place to ensure that Personal Information is being processed responsibly and is not unlawfully accessed.
8. Data Subject participation - the Data Subject must be made aware that their information is being processed and must have provided their informed consent to such processing.

5.1.2 Personal Information may only be processed for a specific purpose. The purposes for which USM Processes or will Process Personal Information, is set out below:

- Administration.
- Rendering services according to contractual agreements.
- Staff administration.
- Complying with all applicable legislation.

5.2 DATA SUBJECTS, INFORMATION PROCESSED AND DUTY OF CARE

5.2.1 A Data Subject may either be a natural or a juristic person. The table below sets out the information that is processed by Data Subject:

Data Subject	**Information Processed**
Clients – Natural Persons	Names, contact details, postal address, date of birth, ID number, tax related information, nationality, gender, confidential correspondence.
Clients – Juristic Persons / Entities	Names of contact persons, name of legal entity, physical and postal address and contact details, registration number, founding documents, tax related information, authorised signatories.
Service Providers	Names of contact persons; name of legal entity, physical and postal address and contact details, registration number, founding document, tax related information, authorised signatories, beneficiaries, ultimate beneficial owners.
Vendors	Names of contact persons; name of legal entity, physical and postal address and contact details, registration number, founding document, tax related information, authorised signatories, beneficiaries, ultimate beneficial owners.
Employees / Directors	Gender, pregnancy, marital status, ethnicity, age, language, education information, financial information, employment history, ID number, physical and postal address, contact details, criminal behaviour, well-being.

5.2.2 USM employs technology to ensure the confidentiality, integrity, and availability of the Personal Information under its care, which includes

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control
- Secure setup of hardware and software making up the IT infrastructure

5.3 CROSS BORDER PERSONAL INFORMATION TRANSFERS

5.3.1 USM does not currently undertake any cross-border transfers of any Personal Information relating to employees, clients, companies, or organisations. USM continually assesses the suitability of the information security measures implemented in order to ensure that the Personal Information that is processed by USM is safeguarded.

6 PAIA AND POPI - REQUEST PROCEDURE

6.1 PAIA – REQUEST FOR INFORMATION

6.1.1 No request shall be accepted verbally nor shall any information be supplied verbally.

6.1.2 A requester must comply with all the procedural requirements contained in the PAIA relating to a request for access to an information record.

6.1.3 A requester must complete the request form enclosed herewith in ANNEXURE 2 and submit it, as well as the payment of a request fee (if applicable) to the Information Officer at the physical address, or electronic mail address as stated herein.

6.1.4 If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the Information Officer.

6.1.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the Information Officer, who shall complete the prescribed form on their behalf.

6.2 POPIA - REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION

6.2.1 No request shall be accepted verbally nor shall any information be supplied verbally.

6.2.2 Section 24 of the POPIA provides that a Data Subject may request for their Personal Information to be corrected/deleted.

6.2.3 A requester must complete the request form enclosed herewith in ANNEXURE 3 and submit it to the Information Officer at the physical address, or electronic mail address as stated herein.

6.2.4 If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the Information Officer.

6.2.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the Information Officer, who shall complete the prescribed form on their behalf.

6.3 POPIA – REQUEST TO OBJECT TO THE PROCESSING OF PERSONAL INFORMATION

6.3.1 No request shall be accepted verbally nor shall any information be supplied verbally.

6.3.2 Section 11 (3) of the POPIA provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information.

6.3.3 A requester must complete the request form enclosed herewith in ANNEXURE 4 and submit it to the Information Officer at the physical address, or electronic mail address as stated herein.

6.3.4 If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the Information Officer.

6.3.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the Information Officer, who shall complete the prescribed form on their behalf.

6.4 PAIA AND POPIA – USM PROCEDURE TO HANDLE REQUESTS AND OBJECTIONS

6.4.1 Only the Information Officer appointed by USM shall have a mandate to decide if a request has been granted or denied.

6.4.2 USM should ordinarily process a request within 30 days, unless the requestor has stated special reasons which would satisfy the Information Officer that circumstances dictate that this period not be complied with.

6.4.3 The USM Information Officer may extend the process for a further 30 days if the request is for a large quantity of information, or the request requires a search for information that has been backup up and stored offsite

and the information cannot reasonably be obtained within the original 30 day period. The Information Officer will notify the requester in writing should an extension be necessary.

6.4.4 If USM has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation from the USM Information Officer. This will include the steps that were taken to try to locate the record.

6.4.5 The following are the grounds on which the USM Information Officer may, subject to the exceptions contained in Chapter 4 of PAIA, refuse a Request for Access in accordance with Chapter 4 of PAIA:

a. Mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of Personal Information would be unreasonable.
b. Mandatory protection of the commercial information of a third party, if the Records contain:
   i. Trade secrets of that third party
   ii. Financial, commercial, scientific, or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party
   iii. Information disclosed in confidence by a third party to USM, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition
   iv. Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.
c. Mandatory protection of confidential information
d. Mandatory protection of the safety of individuals and the protection of property.
e. Mandatory protection of Records that would be regarded as privileged in legal proceedings.
f. Protection of the commercial information of USM, which may include:
   i. Trade secrets, financial/commercial, scientific, or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of USM.
   ii. Information which, if disclosed, could put USM at a disadvantage in contractual or other negotiations or prejudice USM in commercial competition.
   iii. Computer programs which are owned by USM, and which are protected by copyright and intellectual property laws.
g. Research information of USM or a third party, if such disclosure would place the research or the researcher at a serious disadvantage.
h. Requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.
i. If disclosure of the record would prejudice or impair the security of property or means of transport.
j. If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection program.

6.4.6 If a request for information under the PAIA is declined for any reason, the Information Officer shall provide the reasons for the decision, inclusive of the relevant provisions in the PAIA.

6.4.7 If a request for the correction, deletion or objection to the use of Personal Information under POPIA is not agreed to, and if the Data Subject so requests, the Information Officer must take steps as are reasonable in the circumstances to attach to the information in question in such a manner that it will always be read with the additional information that a correction was requested but not made.

6.4.8 If a request for a correction, deletion or objection to the use of Personal Information under POPIA is agreed to where the changed information has an impact on decisions that have been and will be taken in respect of the Data Subject in question, the Information Officer must, if reasonably practicable, inform the Data Subject and each person or body or responsible party to whom the Personal Information has been disclosed of those impacts.

6.5 REMEDIES AVAILABLE TO THE REQUESTER UPON REFUSAL

6.5.1 USM does not have internal appeal procedures. As such, the decision made by the Information Officer is final, and Requesters will have to exercise such external remedies at their disposal if the Request for Access is refused.

6.5.2 In accordance with sections 56(3) (c) and 78 of PAIA, a Requestor may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

7 INCIDENT RESPONSE PLAN (IRP)

7.1 PREAMBLE

7.1.1 This IRP deals with security compromises in respect of Personal Information (PI). The objective is to mitigate potential prejudice to data subjects.

7.2 STATUTORY PROVISIONS

7.2.1 Notification of security compromises is detailed in Section 22 of the POPI Act

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

7.2.2.1 the Information Regulator; and
7.2.2.2 subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

7.2.3 The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

7.2.4 The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

7.2.5 The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

7.2.5.1 mailed to the data subject's last known physical or postal address;
7.2.5.2 sent by e-mail to the data subject's last known e-mail address;
7.2.5.3 placed in a prominent position on the website of the responsible party;
7.2.5.4 published in the news media; or
7.2.5.5 as may be directed by the Regulator.

7.2.6 The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

7.2.6.1 a description of the possible consequences of the security compromise;
7.2.6.2 a description of the measures that the responsible party intends to take or has taken to address the security compromise;
7.2.6.3 a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
7.2.6.4 if known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information.

7.3 INCIDENT RESPONSE TEAM (IRT)

7.3.1 The IRT shall take steps to identify and deal with threats and the safeguards required to maintain secure systems.

7.3.2 The IRT shall comprise the Information Officer (Team Lead), the Human Resources Executive and other co-opted members as required.

7.3.3 The IRT Lead shall consider the following in deciding an appropriate response to an incident –

7.3.3.1 Based on the merits of each incident, decide which of the IRT members shall be engaged;
7.3.3.2 Assigning clear responsibilities and priorities across IRT members;
7.3.3.3 Managing all internal and external stakeholder interests and engagements, including executive management, external business and statutory parties;
7.3.3.4 Ensure that incidents are documented in detail;
7.3.3.5 Ensure that all statutory and company obligations are addressed.

7.4 TRAINING

7.4.1 Every manager and employee should be aware of the provisions of the POPI Act, their responsibilities in this regard and prepared to participate in an effective and agile incident response plan.

7.4.2 POPI and personal information security training should be conducted annually

7.5 IMPACT ASSESSMENT

7.5.1 In order to prevent the loss of or damage to personal information, USM shall:

7.5.1.1 Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
7.5.1.2 Establish and maintain appropriate safeguards against the risks identified;
7.5.1.3 Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

7.5.2 ANNEXURE 5 provides an impact assessment guideline to be used in identifying, describing, improving and managing risks. Impact assessments should be conducted when significant change has occurred within the company or external environment that may increase risk exposure.

7.6 DATA AND SECURITY BREACHES

7.6.1 Data breaches include:

7.6.1.1 Loss or theft of hard copy documents or files
7.6.1.2 Loss or theft of USB drives, computers or mobile devices
7.6.1.3 An unauthorised person gaining access to a laptop, email account or a computer network
7.6.1.4 Sending an email with personal data to the wrong person
7.6.1.5 A disgruntled employee copying a list of contacts for their personal use
7.6.1.6 Passwords hacked or revealed
7.6.1.7 Computers infected with a virus or malware
7.6.1.8 Servers compromised
7.6.1.9 Cyber and ransomware attacks
7.6.1.10 Database hacking
7.6.1.11 Phishing

7.6.2 Security breaches include:

7.6.2.1 An attack on a vulnerable system due to it being outdated from an operating system viewpoint;
7.6.2.2 Weak passwords which can be cracked or guessed;
7.6.2.3 Malware attacks, such as phishing emails;
7.6.2.4 Social engineering where, for example, an intruder phones an employee claiming to be from the IT helpdesk and asks for the password in order to repair the computer;
7.6.2.5 Firewall Breach
7.6.2.6 Virus Outbreaks.

7.6.3 All data and security breaches must be reported to the IRT lead. If there are reasonable grounds to believe that the personal information of a data subject has been compromised, the responsible party must notify the regulator and the data subjects.

7.7 INCIDENT RESPONSE PLAN – DATA BREACH OF PERSONAL INFORMATION

7.7.1 The IRT Lead will be the central point of contact for reporting any suspected or confirmed breach of personal information.

7.7.2 The IRT Lead will document each alleged, suspected and/ or verified breach of personal information and will assign a case number.

7.7.3 The IRT Lead shall as soon as is reasonable possible ensure that the necessary steps are taken to contain and control the incident to prevent further unauthorized access to or use of personal information.

7.7.4 The IRT Lead shall, with the support of the appropriate IRT members, monitor systems and the network for signs of continued intruder access. It is important to preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. All actions taken need to be documented; by whom and the exact time and date.

7.7.5 The IRT lead will compile a detailed report and submitted to the CEO within 48 hours of the breach being identified, which shall contain the following information

7.7.5.1 How the breach occurred?
7.7.5.2 The extent and materiality of the data breach?
7.7.5.3 Interim measures put in place to prevent further compromise?
7.7.5.4 Security measures put in place to prevent a recurrence of such a breach?
7.7.5.5 Measures that should be taken to inform the data subjects so that they can take proactive measures against the potential consequences of the compromise.

7.7.6 The IRT Lead shall immediately share the above report with the CEO and together they must decide the way forward, which may include the following:

7.7.6.1 Notification of the Information Regulator (not later that a total of 48 hours after having identified the breach).

7.7.6.2 Notification of data subjects whose personal information has been breached (not later that a total of 48 hours after having identified the breach).

7.7.6.3 To engage appropriate authorities (Chairman of the Board, Audit and Risk Committee, etc) and advisors (attorneys etc) to ensure that the interests of the company and its stakeholders are addressed;

7.7.6.4 To initiate criminal investigations and other actions as appropriate.

ANNEXURE 1: PAIA - APPLICABLE FEES IN RESPECT OF PRIVATE BODIES

Fees in Respect of Private Bodies

Item	Description	Amount
1.	The request fee payable by every requester	R140.00
2.	Photocopy/printed black & white copy of A4-size page	R2.00 per page or part thereof.
3.	Printed copy of A4-size page	R2.00 per page or part thereof.
4.	For a copy in a computer-readable form on: (iii) Flash drive (to be provided by requestor) (iv) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60.00
5.	For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on quotation from Service provider.
6.	Copy of visual images	
7.	Transcription of an audio record, per A4-size page	R24.00
8.	Copy of an audio record on: (v) Flash drive (to be provided by requestor) (vi) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60.00
9.	To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation. To not exceed a total cost of	R145.00 R435.00
10.	Deposit: If search exceeds 6 hours	One third of amount per request calculated in terms of items 2 to 8.
11.	Postage, e-mail or any other electronic transfer	Actual expense, if any.".

ANNEXURE 2: PAIA - FORM REQUESTING ACCESS TO A RECORD

Request For Access To Record of Private Body
Section 53(1) of the Promotion of Access to Information Act, 2000 Act No. 2 of 2000; Regulation 10

A. Particulars of a Private Body
The Head:

B. Particulars of Person Requesting access to the Record

a) The particulars of the person who requests access to the record must be given below.
b) The contact details in the Republic of South Africa to which the information is to be sent must be given.
c) Proof of the capacity in which the request is made, if applicable, must be attached.

i. Full Names and Surname: _____
ii. Identity Number: _____
iii. Postal Address: _____
iv. Email Address: _____
v. Telephone Number: _____
vi. Capacity in which request is made when made on behalf on another person: _____

C. Particulars of Person on whose behalf request is made

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

Full Names and Surname: _____
Identity Number: _____

D. Particulars of Record

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

i. Description of record or relevant part of the record: _____
ii. Reference Number, if available: _____
iii. Any further particulars of the record _____

E. Fees

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

d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.

i. Reason for exemption from payment of fees: _____

F. Form of Access to Record

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

i. Disability: _____
ii. Form in which Record is required:: _____

iii. Mark the appropriate box with an X.

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

iv. If the Record is in written or printed form

Copy of Record required ☐ or Inspection of Record of Record required ☐

v. If record consists of visual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):

View the Images ☐ Copy of the Images* ☐ Transcription of the Images* ☐

vi. If record consists of recorded words or information which can be reproduced in sound:

Listen to the soundtrack (audio cassette, CD, DVD, or digital audio format) ☐
Transcription of soundtrack* (written or printed document) ☐

vii. If record is held on computer or in an electronic or machine-readable form:

Printed copy of record* ☐
Printed copy of information ☐
Derived from the record* ☐
Copy in computer readable form* (CD, DVD, or digital audio format) ☐

viii. *If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable ☐

G. Particulars of right to be exercised or protected

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

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

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

H. Notice of decision regarding request for access

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

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

Signed at _____ this _____day_____ of 20_____

_____
Signature of Requester/Person on whose behalf request is made

Once completed this form should be sent to the USM Information Officer.

ANNEXURE 3: POPIA - FORM REQUESTING AMENDMENT, CORRECTION OR DELETION OF PERSONAL DATA

Request for Amendment, Correction or Deletion of Personal Information
Section 24 (1) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) and Regulations Relating to the Protection of Personal Information, 2017 Regulation 3 (2)

Section 24 (1) of POPI and regulation 3 of the POPI Regulations provides that a Data Subject may request for their Personal Information to be amended / corrected / deleted as held by us.

As a main rule, your request will be handled free of charge. However, if we were to find your request to be manifestly unfounded, excessive, or repetitive, we may charge a reasonable fee based on the administrative cost of amending / correcting / deleting the information.

Please fill out the details below and we will get back to you 30 calendar days upon receipt of a fully completed form, proof of identity and other required documents, if applicable. The aforementioned documentation should be sent to the USM Information Officer.

Details of the person requesting correction / deletion	
Full name:	
Address:	
Date of Birth:	
Email Address:	
Phone Number:	

Your role	
☐	I am the data subject.
☐	I am not the data subject and I am acting on behalf of the data subject by virtue of a power of attorney.
☐	I am not the data subject and I am acting on behalf of the data subject as its parent or legal guardian.

Proof of Identity and Authority Submitted	
☐	Driving licence.
☐	Passport.
☐	Identity Document.
☐	Power of Attorney.
☐	Evidence of parental responsibility or legal guardianship

Amendment	
☐	I wish to amend my personal data (proof of identity must be provided).
☐	I wish to amend personal data concerning a data subject that I am acting on behalf of (proof of identity of the representative, a power of attorney and proof of identity of the data subject must be provided).
☐	I wish to amend personal data concerning a data subject to whom I am a parent or legal guardian (proof of identity and evidence of parental responsibility or legal guardianship must be provided).

Type of personal data you wish to amend:	
Describe the amendment:	
State the reasons for the amendment.	

Correction	
☐	I wish to correct my personal data (proof of identity must be provided).
☐	I wish to correct personal data concerning a data subject that I am acting on behalf of (proof of identity of the representative, a power of attorney and proof of identity of the data subject must be provided).
☐	I wish to correct personal data concerning a data subject to whom I am a parent or legal guardian (proof of identity and evidence of parental responsibility or legal guardianship must be provided).
Type of personal data you wish to correct:	
Describe the correction:	
State the reasons for the correction.	

Deletion	
☐	I wish to delete my personal data (proof of identity must be provided).
☐	I wish to delete personal data concerning a data subject that I am acting on behalf of (proof of identity of the representative, a power of attorney and proof of identity of the data subject must be provided).
☐	I wish to delete personal data concerning a data subject to whom I am a parent or legal guardian (proof of identity and evidence of parental responsibility or legal guardianship must be provided).
Type of personal data you wish to delete:	
Describe the deletion:	
State the reasons for the deletion.	

By signing this form, you certify that the information you have provided is correct to the best of your knowledge and that you are the person to whom it relates or that you are legally entitled to act on behalf of such person. You understand that it may be necessary to obtain further information in order to comply with this request.

Signed at _____ this _____day_____ of 20_____

_____
Signature of Requester/Person on whose behalf request is made

Once completed this form should be sent to the USM Information Officer.

ANNEXURE 4: POPIA - FORM TO OBJECT TO THE PROCESSING OF PERSONAL INFORMATION

Objection To The Processing Of Personal Information In Terms Of Section 11(3) Of The Protection Of Personal Information Act, 2013 (Act No. 4 Of 2013)
Regulations Relating To The Protection Of Personal Information, 2017, Regulation 2(1)

Please Note:
a. Affidavits or other documentary evidence in support of the object needs to be attached to this form.
b. If more space is required add additional pages as appendices to this form.

Details of the Data Subject	
Full name:	
Address:	
Date of Birth:	
Email Address:	
Phone Number:	

Details of the Responsible Party	
Full name:	
Address:	
Date of Birth:	
Email Address:	
Phone Number:	

Reasons for Objection (Please provide full details)

Signed at _____ this _____day_____ of 20_____

_____
Signature of Requester/Person on whose behalf request is made

Once completed this form should be sent to the USM Information Officer.

ANNEXURE 5: POPIA – IMPACT ASSESSEMENT GUIDELINE