PAIA MANUAL

PROMOTION OF ACCESS TO INFORMATION

COMPILED IN TERMS OF THE PAIA ACT, NO 2 OF 2000

FOR

SURGO (PTY) LTD

TABLE OF CONTENTS

1) DEFINITIONS

PAIA means the Promotion of Access to Information Act 2 of 2000 (as Amended)

POPIA means the Promotion of Personal Information Act 4 of 2013

Information Regulator means the Regulator established in terms of Section 39 of POPIA

Person means a natural person or a juristic person

Private body means:

- a natural person who carries or has carried on any trade, business or profession, but only in such capacity
- a partnership which carries or has carried on any trade, business or profession; or
- any former or existing juristic person, but excludes a public body

Public body means:

- any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
- any other functionary or institution when:
  - exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
  - exercising a public power or performing a public function in terms of any legislation

Head, in relation to, a private body means:

- in the case of a natural person, that natural person or any person duly authorised by that natural person;
- in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
- in the case of a juristic person:
  - the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
  - the person who is acting as such or any person duly authorised by such acting person

Information Officer (IO) means the head of a private body

Deputy Information Officer (DIO) means the person to whom any power or duty conferred or imposed on an Information Officer by POPIA has been delegated

Requester in relation to a private body**,** means any person, including, but not limited to public body or an official thereof, making a request for access to a record of the organisation or a person acting on behalf of such person

Personal Requester means a requester seeking access to a record containing personal information about the requester

Personal Information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail 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; and 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

Request for access means a request for access to a record of the organisation in terms of section 50 of PAIA

Record means any recorded information regardless of the form or medium, in the possession or under the control of the organisation irrespective of whether or not it was created by the organisation

Data Subject means the person to whom personal information relates

Third Party in relation to a request for access to a record held by the organisation, means any person other than the requester

Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including 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 restriction, degradation, erasure or destruction of information

2) PURPOSE OF A PAIA MANUAL

The Promotion of Access to Information Act, 2000, gives effect to section 32 of the Constitution, which provides that everyone has the right to access information held by the State or any other person (or private body), when that information is required for the exercise or protection of any rights.

The purpose of PAIA is to:

- foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information, and to

- actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights

The organisation recognises everyone's right to access information and is committed to providing access to the organisation's records where the proper procedural requirements as set out by PAIA and POPIA have been met.

The organisation's PAIA manual is compiled in accordance with section 51 of the Act.

3) INFORMATION OFFICER

The Director, **Rudé Alley**, is the designated Information Officer of **SURGO (PTY) LTD**. The contact details of the Information Officer are as follows:

A. Head of Organisation – Information Officer

Full names & surname:	Rudé Alley
Email address:	rude@surgo.co.za
Phone number:	+27 21 012 5566

The Information Officer has, in terms of section 17 of the Act, delegated his powers under PAIA to the following Deputy Information Officers:

B. Deputy Information Officers

Full names & surname	Madre Cordy
Email address:	madre@surgo.co.za
Phone number:	+27 21 012 5566

The Information Officer and the Deputy Information Officers share the same physical and postal address as below:

C. Organisation Contact Details

Postal address:	47 Ocean Spirit Ave, Sanddrift, Cape Town, 7441, SA
Street address:	n/a (fully remote)
Phone number:	+27 21 012 5566
Website:	www.surgo.co.za

D. Business Type

The organisation conducts its main type of business in the following sector(s):
BPO Industry, HR & Recruitment

4) PAIA GUIDE

Requesters are referred to the guide in terms of section 10 of the Act which has been compiled by the Information Regulator (South Africa). The guide contains information for the purposes of exercising Constitutional rights. Requests in terms of PAIA shall be made in accordance with the prescribed procedures at the rates provided.

The guide is available in all South African official languages free of charge and any person may request a copy of the guide.

A copy of the guide may be obtained by contacting the Information Regulator (South Africa) at:

- Postal Address: **The Information Regulator (South Africa) PO Box 31533, Braamfontein, Johannesburg, 2017**
- Telephone Number: **+27(0)10 023 5200**
- Website**:** **www.inforegulator.org.za**
- Email: **enquiries@inforegulator.org.za**

5) CATEGORIES OF RECORDS HELD

The organisation maintains statutory records and information in terms of the following legislation:

Basic Conditions of Employment Act 75 of 1997
Companies Act 71 of 2008
Compensation of Occupational Injuries & Diseases Act 130 of 1993
Consumer Protection Act 68 of 2008
Consumer Affairs (Unfair Business Practices) Act 71 of 1988
Copyright Act 98 of 1978
Credit Agreements Act 75 of 1980
Employment Equity Act 55 of 1998
Finance Act 35 of 2000
Financial Relations Act 65 of 1976
Harmful Business Practices Act 23 of 1999
Insolvency Act 24 of 1936
Intellectual Property Laws Amendments Act 38 of 1997
Labour Relations Act 66 of 1995
National Credit Act 34 of 2005
Occupational Health and Safety Act 85 of 1993
Protection of Personal Information Act 4 of 2013
Skills Development Levies Act 9 of 1999
Skills Development Act 97 of 1998
Trademarks Act 194 of 1993
Unemployment Contributions Act 4 of 2002
Unemployment Insurance Act 63 of 2001
Value Added Tax Act 89 of 1991

6) AVAILABILTY OF RECORDS

The organisation maintains the following categories of records and related subject matter. The status of the record's availability, the purpose for its processing and the relevant data subject category to who the record relates are set out below:

Category:	Record:	Availability:	Purpose:	Data Subject:
Public Affairs	Public Product Information	Freely Available	Convey Public Information	Organisation
	Public Corporate Records	Freely Available	Convey Public Information	Organisation
	Media Releases	Freely Available	Convey Public Information	Organisation
	Published Newsletters	Freely Available	Convey Public Information	Organisation
Regulatory & Administrative	Permits, Licenses or Authorities	Freely Available	Statutory Requirement	Organisation
	Memorandum of Incorporation	PAIA Request	Statutory Requirement	Organisation
	Register of Members	PAIA Request	Statutory Requirement	Organisation
	Register of Board of Directors	PAIA Request	Statutory Requirement	Organisation
	Internal correspondence (e-mails/memos)	PAIA Request	Internal Communications	Employees

	Insurance Policies held by organisation	PAIA Request	Risk Management	Organisation
Human Resources	Employment Applications	PAIA Request	Internal Referencing	Employees
	Employment Contracts	PAIA Request	Contractual Agreement	Employees
	Personal Information of Employees	PAIA Request	Internal Referencing	Employees
	Employment Equity Plan	PAIA Request	Statutory Requirement	Organisation
	Disciplinary Records	PAIA Request	Statutory Requirement	Employees
	Performance Management Records	PAIA Request	Internal Referencing	Employees
	Salary Records	PAIA Request	Internal Referencing	Employees
	PAYE Records	PAIA Request	Statutory Requirement	Employees
	SETA Records	PAIA Request	Statutory Requirement	Employees
	Disciplinary Code	PAIA Request	Statutory Requirement	Organisation
	Leave Records	PAIA Request	Internal Referencing	Employees
	Training Records	PAIA Request	Internal Referencing	Employees
	Training Manual	PAIA Request	Internal Referencing	Organisation
Financial	Financial Statements	PAIA Request	Internal Referencing	Organisation
	Financial and Tax Records	PAIA Request	Statutory Requirement	Organisation
	Asset Register	PAIA Request	Internal Referencing	Organisation
	Management Accounts and Reports	PAIA Request	Internal Referencing	Organisation
	Vouchers, Cash Books and Ledgers	PAIA Request	Internal Referencing	Organisation
	Banking Records and Statements	PAIA Request	Internal Referencing	Organisation
	Electronic Banking Records	PAIA Request	Internal Referencing	Organisation
Marketing	Market Information	PAIA Request	Internal Referencing	Organisation
	Product Brochures	PAIA Request	Internal Referencing	Organisation
	Performance Records	PAIA Request	Internal Referencing	Organisation
Client Customer	Customer / Client Database	PAIA Request	Internal Referencing	Customers
	Customer / Client agreements	PAIA Request	Internal Referencing	Customers
	Customer / Client Files	PAIA Request	Internal Referencing	Customers
	Customer / Client Instructions	PAIA Request	Internal Communications	Customers
	Customer / Client Correspondence	PAIA Request	External Communications	Customers
Third Party	Rental agreements	PAIA Request	Contractual Agreement	Third Party
	Non-disclosure agreements	PAIA Request	Risk Management	Third Party
	Letters of Intent	PAIA Request	Contractual Agreement	Third Party
	Supplier Contracts	PAIA Request	Contractual Agreement	Third Party

7) PURPOSE OF PROCESSING PERSONAL INFORMATION

PURPOSE OF PROCESSING PERSONAL INFORMATION

We process personal information for a variety of purposes, including but not limited to the following:

- *To provide or manage any information, products and/or services requested by data subjects;*
- *To help us identify data subjects when they contact the company;*
- *To maintain customer records;*
- *For recruitment purposes;*
- *For general administration, financial and tax purposes;*
- *For legal or contractual purposes;*
- *To help us improve the quality of our products and services;*
- *To help us detect and prevent fraud and money laundering;*
- *To help us recover debts;*
- *To carry out analysis and customer profiling;*
- *To facilitate travel for business purposes;*
- *To fulfil a contractual obligation to a shareholder or to fulfil a contractual obligation to a thrid party;*
- *To enable suppliers to provide goods or services to us and receive payment for these goods or services and collect information for B-BBEE reporting and accreditation purposes.*
- *To fulfil statutory obligations in terms of the Companies Act, 71 of 2008 (directors' information);*
- *To assess applications and onboard new clients or service providers or suppliers;*
- *To compile offer letters or expressions of interest;*
- *To do due-diligence assessments;*
- *To do yearly or periodic reviews or due-diligence assessments of clients and service providers or suppliers;*
- *Engage in general correspondence.*

DESCRIPTION OF THE CATEGORIES OF DATA SUBJECTS AND OF THE INFORMATION OR CATEGORIES OF INFORMATION RELATING THERETO

Specify the categories of data subjects in respect of whom the body processes personal information and the nature or categories of the personal information being processed.

Categories of Data Subjects	***Personal Information that may be processed***
Customer / Clients	Names, surnames, address, registration numbers / identity numbers, employment status, bank details
Service Providers	Names, registration number, vat number, address, trade secrets, bank details
Employees	Names, surnames, address, identity number, qualifications and professional registrations, gender, race, bank details, contact details, CVs, tax information, marital status, citizenship, next of kin, and training records.
Suppliers	Name, address, company registration numbers, tax numbers, PAYE numbers, banking details, and contact details.

THE RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL INFORMATION MAY BE SUPPLIED

Specify the person or category of persons to whom the body may disseminate personal information.

Category of personal information	**Recipients / Categories of Recipients to whom the personal information may be supplied**
Identity number and names for criminal checks	South African Police Services
Qualifications, for qualification verification	South African Qualifications Authority
Credit and payment history, for credit information	Credit Bureaus
B-BBEE	B-BBEE assessment or verification agency
Employee names, identity numbers and demographics	SETA (for programs)
Identity number, names, employee numbers, contact details, employment dates, statutory requirements (including tax) and salary information	• Department of Labour (UIF) • South African Revenue Service (PAYE, SDL, UIF) • Commission for Conciliation, Mediation and Arbitration (labour relations) • Reference checks for former employees.

PLANNED TRANSBORDER FLOWS OF PERSONAL INFORMATION

We want to affirm that Surgo does not engage in any transborder flows of personal information. All data we collect, process, and store is confined exclusively within the borders of South Africa.

GENERAL DESCRIPTION OF INFORMATION SECURITY MEASURES

- We are compliant with ISO/IEC 27001 International Standard on Information Security and GDPR, as a result we have policies in place that govern and ensure safekeeping of information. A list of the most relevant policies and how it relates to safekeeping of data follows below. **Information security policy:**The Information Security Policy provides a framework around which Information Security Objectives can be defined and used to monitor the ongoing achievement of business, client, and information security requirements. Employees may only access information needed to perform their legitimate duties as a Company employee and only when authorised by the appropriate Director, Manager or Information Security Management Officer (ISMO) or person appointed by him/her. **Password Policy**The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 90 days. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days. All user-level passwords are locked after a set number of failed logins equal to 5, JAMF protect works according to an international GDPR compliancy and only allows 5 mistaken login attempts before the computer is locked. All user-level and system-level passwords must conform to the guidelines described in the policy.User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user. Password protected screensavers enabled on each laptop to lock after a short timeout period to ensure that workstations that are left unsecured will be protected. Each user is required to lock their laptop when unattended. **Removable Media Policy**The objective of this policy is to prevent unauthorized disclosure, modification, removal, or destruction of information assets, whether Surgo or client information, and to prevent interruption to business activities. Surgo has specifically removed authorizaiton for the use of Removable Media within the company, however within certain roles and under certain circumstances, removable media may be used. Where this is the case, the following requirements must be adhered to:Unauthorized users are not permitted to use any removable media.
- All removable media drives will be automatically scanned by the Antivirus software.
- Removable media will only be issued to employees who have a clear business need for them. Issue of such media to sub-contractors and temporary workers must be specifically authorized by the IT Manager, failing him or her the Operations Manager may approve the use of Removable Media.
- Removable media may only carry information that is required for a specific purpose, e.g., the retrieval of a client database – in other words, once a purpose has been fulfilled, the information must be erased from the media.
- Media is disposed of securely and as required in the policy for the Disposal of IT Assets Procedure.
- All users that are authorized to use removable media devices, are required to encrypt any removable media using either Bit locker or File Vault. If you are unsure as to the encryption of the device, seek the assistance of the IT Manager

Acceptable use policy

- The Companies Acceptable Use Policy (this document) covers all of Surgo's information assets, including hardware, software, mobile devices and peripherals including memory devices, Tablets, iPads, and mobile phones. It sets out what Surgo considers to be acceptable use of those assets and applies to all employees, contractors, temporary workers and third parties who use, work with or connect to Surgo information processing facilities.

    - Providing access to another individual, either deliberately or through failure to secure your devices access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set as per the Password Policy.
- You must lock the screen or log off when the device is unattended.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware

Mobile device policy

- This policy describes the controls necessary to minimize information security risks affecting Surgo mobile devices including laptops, tablets and mobile phones
    - All Mobile devices that access company data and store company data is required to be encrypted. Windows Devices must use the latest Bitlocker version that is supported by the Windows version installed on the device. Apple laptops and desktops are required to use the latest version of File Vault that is supported by the version of MacOS that has been installed.
- Surgo owned laptops are required to have Bitlocker configured in both TPM and PIN combination.
- Windows Mobile and Apple mobile devices are encrypted by default. You may only access Surgo services by means of Mobile devices that are encrypted. If an older device is found, encryption needs to be verified before allowing access to any Surgo Services.
- Mobile device compliance is managed through Microsoft Exchange MDM. The policy assigned to the devices must match the users Role.

Access control policy

- The objective of this policy is to provide information security requirements to:
- Protect against unauthorized access to computer systems, applications or operating systems owned or maintained by Surgo.
- Allow only authorized users the appropriate level of access to the information or portion of the system, application, or operating system necessary to accomplish designated responsibilities. This policy applies to all systems and applications that utilize an access control system to protect resources from unauthorized access including all development, staging, production, and operational environments.
    - Where appropriate all employees will be subject to pre-employment screening checks. The requirements of such screening will be subject client contractual requirements and will be confirmed prior to commencing employment.
- Access to systems or system function must be limited to only authorized users and conform to best security practices related to Role Based Access Control (RBAC). For all new employees or contractors, Human resources are to notify the IT Department by means of a ticket (or email) with the details of tthe new user.
- Prior to the creation and granting of access privileges, user identities must be subject to an authorization process that tracks and documents access request detail, and final approval
- User identities must be authenticated prior to system access. The Company will use various tools and systems to authenticate users, such as passwords, two factor authentication and Active Directory user activation and authentication.
- In specific cases when misuse of a user identity is suspected, user access must be disabled immediately, and this must be reported to the IT Manager as well as the HR Manager for possible investigation into Information Security Policy disciplinary process.

Anti-malware policy

- The purpose of this policy is to promote the use of anti-virus and other anti-malware software and educate the employees regarding the policies that are widely followed to use anti malware software effectively.
    - All workstations whether connected to the Surgo network, or standalone, must use Surgo-approved anti-virus and anti-malware software and configuration. The approved Anti-Virus and Anti-Malware System is JamF Protect
- Any personal workstation accessing any Surgo resources as part of remote work must use Surgo-approved anti-virus and anti-malware software and configuration
- The information system automatically updates malicious code protection mechanisms e.g., automatic updates of anti-virus and anti-malware software.
- All incoming and outgoing e-mails are to be scanned for malware using the JAMF Protect system that will when anyone tries to download a file that is affected and immediately stop it.

Cryptographic control policy

- The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that regulations are followed.
    - Surgo uses software encryption technology to protect Confidential Information or PII. To provide the highest-level security while balancing throughput and response times, encryption key lengths should use current industry standard encryption algorithms for Confidential Information or PII.
- Symmetric cryptosystem key lengths must be at least 256 bits. Surgo's key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows. The use of proprietary encryption algorithms is not allowed unless reviewed by qualified experts outside of the vendor in question and approved by Surgo management.

Information transfer policy

- The objective of this policy is to provide information security requirements to:
- Ensure all information transferred in and out of the company meets the security protocols and does not breach any confidentiality requirements.

- Protect Surgo data transmitted. The scope of this policy includes all classifications of data, weather internally generated or received from a 3rd party (e.g., Customer).
    - Surgo requires the following types of information to be encrypted when in transit (All customer and personal data) If information is required to be encrypted, it must be protected by a strong password and should never be copied or shared in a way that would make it available outside of the encryption process, For data that is not encrypted there is safe ways on that is used for other processes as well.
- Data must only be transferred via secure protocols i.e., SFTP, MFTP, FTPS and may not be transferred with less secure protocols i.e., FTP. Data is not allowed to be transferred without the permission of the client or management and for the purposes of intended use

Network security policy

- The purpose of this policy is to provide the procedures and policy requirements for Network management and connection of systems both internal within Surgo, and externally to the internet and or Clients System. There is currently no internal or local area or wide area network at Surgo. As the business is currently configured for remote or mobile working, the following procedures and systems are in place:
- All Staff have been issued with mobile network routers provided for by SURGO.
- Staff has been allocated with fiber allowance, each staff member that has submitted the signed form that opted for a allowance is receiving funds for their Fiber connection and is liable for their own connection.
- All staff will connect to the Internet via the mobile network routers connecting to the nearest Vodacom and MTN tower which will route the connection to the main tower connecting to the Internet.
- All Routers are connected using a unique encrypted password provided by Vodacom and MTN.
- The JAMF system locks down each connection and does not allow sharing capabilities to other devices.
- Client systems are protected by a SSO Provider with multi factor authentication via OKTA (www.okta.com)
- Any changes to the Network requirements will be processed through the Change Management procedure and have full Management Approval.

Technical vulnerability and patch policy

- The goal of vulnerability and patch Management is to keep the components that form part of information technology infrastructure (hardware, software, and services) up to date with the latest patches and updates
    - All of the hardware and software on the organization's network will be scanned using a vulnerability scanner to identify weaknesses in the configuration of systems and to determine if any systems are missing important patches, or software such as anti-virus software. The organization's network will be scanned at a minimum on a quarterly basis. Remediation will be undertaken of any vulnerabilities identified.
- The organization's anti-virus server will be configured to automatically download the latest virus and spyware definitions and push them to the servers, PC's and tablets running on the network. Windows patch management tools will be utilized to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate. Security weaknesses and software update notifications issued by Computer Emergency Response Teams (CERT) will be monitored on a regular basis and any critical issues affecting the organization's IT infrastructure will be attacked upon immediately.

Remote working policy

- The objective of this Policy is to provide information security requirements to help ensure that information Security is not compromised on Surgo Information Systems and to satisfy all relevant compliance and regulatory commitment as it relates to best practices and general IT governance controls.
    - A designated workspace should be maintained by the employee in a clean, professional, and safe condition.
- Should you work at a public location for any reason, then you are obliged to ensure that no one can see what is on your screen in order to protect our clients' information, failure of which, may constitute a GDPR breach.

Disciplinary policy

- Information security breaches are dealt with as a dismissal with first offence.

Digital monitoring and tracking policy

- This policy refers to the monitoring and tracking of all digital data / platforms used on company equipment and utilized by the employees of Surgo (Pty). In terms of the legal requirements referred to in the GDPR (General Data Protection Regulation), the company reserves the right to monitor and track all digital activity, such as work performance data, emails and any other systems / digital platforms owned/not owned by the company.
- Further to the policies we conduct regular mandatory information security training and internal vulnerability tests to ensure employees are educated and vigilant to any possible cyber-attacks.
- To monitor adherence, we make use of monitoring software that is installed on the employee's device. The software cannot be altered or removed by the employee and is solely controlled by authorized members of our technical team. This software captures actions and steps taken and take frequent screen recordings. Furthermore, we have our own timekeeping solution to track employee tasks and actions.

8) REQUEST PROCEDURE

To facilitate the processing of your request, kindly complete and submit Form A which is attached to this manual as Annexure A. The request form must be addressed to the Deputy Information Officer using the contact details set out in clause 3 above.

The Deputy Information Officer will notify the requester that a request for access has been received and that the prescribed fee (if any) is payable prior to processing the request. Please refer to Annexure B for a full breakdown of fees payable. Personal requesters will not be charged a request fee.

Once the request has been processed, the Deputy Information Officer will inform you of the outcome of your request and any additional fees that may fall due.

Please be advised that PAIA provides a number of grounds on which a request for access to information must be refused. These grounds mainly comprise instances where:

- the privacy and interests of other individuals are protected
- where such records are already otherwise publicly available
- instances where public interest are not served
- the mandatory protection of commercial information of a third party
- the mandatory protection of certain confidential information of a third party

When completing the form below please:

- indicate the identity of the person seeking access to the information
- provide sufficient particulars to enable the deputy information officer to identify the information requested
- specify the format in which the information is required
- indicate the contact details of the person requiring the information
- indicate the right to be exercised and/or to be protected, and specify the reasons why the information required will enable the person to protect and/or exercise the right
- where the person requesting the information wishes to be informed of the decision of the request in a particular manner, state the manner and particulars to be so informed
- if the request for information is made on behalf of another person, submit proof that the person submitting the request, has obtained the necessary authorisation to do so

9) RIGHT OF ACCESS

The Information Officer and/or Deputy Information Officer may only provide access to any record held by the organisation to a requester if:

- The record is required for the exercise or protection of any right, and
- The requester complies with the procedural requirements relating to a request for access to that record, and
- Access to that record is not refused in terms of any of the grounds for refusal

10) DECISION FOR REFUSAL

The Information Officer and/or Deputy Information Officer must assess whether there are any grounds for refusing a request for access. Where any grounds for refusal are found, a request for access will not be granted. The requester shall be notified of the company's decision, in the most reasonable manner possible.

In the event where the access to information is refused, the requester shall be provided with a written reason for such refusal.

11) RIGHT TO CHALLENGE

If a requester does not agree with the decision of the company, the requester may lodge a complaint with the Information Regulator or an application with a court against the refusal of the request, and the procedure (including the period) for lodging a complaint with the Information Regulator or the application

12) MANUAL REVIEW

This manual is a working document and will be reviewed periodically but no less than once a year.

ANNEXURE A : REQUEST FORM

A. Particulars of Private Body	
The Head:	
B. Particulars of person requesting access to the record	
(i) The particulars of the person who requests access to the record must be recorded below (ii) Furnish an address and/or fax number in the Republic to which information must be sent (iii) Proof of the capacity in which the request is made, if applicable, must be attached	
Full names & surname:	
Identity number:	
Postal address:	
Fax number:	
Telephone number:	
Email address:	
Capacity:	
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 & surname:	
Identity number:	
D. Particulars of Record	
(i) Provide full particulars of the record to which access is requested, including the reference number if that is known to you (ii) If the provided space is inadequate, please continue on a separate page and attach to this form. Please sign any additional pages	
Description of record:	
Reference number:	
Any further particulars:	
E. Fees	
(i) 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 (ii) You will be notified of the amount required to be paid as the request fee (iii) 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	

(iv) If you qualify for exemption of the payment of any fee, please state the reason therefor	
Reason for exemption:	

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 hereunder, please state your disability and indicate in which form the record is required	
Disability:	
Form in which required:	

Mark the appropriate box with an "X"	
(i) Your indication as to the required form of access depends on the form in which the record is available	
(ii) Access in the form requested may be refused in certain circumstances, In such a case you will be informed of access will be granted in another form	
(iii) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested	
1) If the record is in written or printed form:	
▪ copy of record	
▪ inspection of record	
2) If record consists of visual images:	
▪ view the images	
▪ copy of the images	
▪ transcription of the images	
3) If the record consists of recorded words or information which can be reproduced in sound:	
▪ listen to the soundtrack	
▪ transcription of the soundtrack	
4) If the record is held on computer or in an electronic or machine-readable form:	
▪ printed copy of record	
▪ copy in computer readable form	
Please indicate the preferred method of delivery	
▪ By hand	
▪ Email	
▪ Post	
▪ Fax	

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 additional folios.	
Indicate which right is to be exercised or protected:	

Explain why the record requested is required for the exercise or protection of the aforementioned right:
H. Notice of decision regarding the request for access
You will be notified in writing whether your request has been approved / denied. If you wish to be informed thereof in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request
How would you prefer to be informed of the decision regarding your request for access to the record?
I. Signature page
Signed at:
Date:
Signature of Requester / Person on whose behalf request is made:

ANNEXURE B: PRESCRIBED FEES

The following applies to requests (other than personal requests):

- A requester is required to pay a preliminary request fee before a request will be processed
- If the preparation of the record requested requires more than the prescribed hours (six), an additional deposit shall be paid (of not more than one third of the access fee which would be payable if the request was granted)
- A requestor may lodge an application with a court against the render / payment of the request fee and/or deposit
- Records may be withheld until the fees have been paid
- The fee structure is also available on the South African Human Rights Commission's website at www.sahrc.org.za

No.	Description	Fee
1.	The fee for a copy of the manual as contemplated in regulation 9(2)(c), for every photocopy of an A4-size page or part thereof	R1.10
2.	The fees for reproduction referred to in regulation 11(1) are as follows:	-
	a) For every photocopy of an A4 size page or part thereof	R1.10
	b) For every printed copy of an A4 size page or part thereof held on a computer or in electronic readable form	R0.75
	c) For a copy in a computer-readable form on stiffy disc	R7.50
	d) For a copy in a computer-readable form on compact disc	R70.00
	e) For a transcription of visual images, for an A4 size page or part thereof	R40.00
	f) For a copy of a visual image	R60.00
	g) For a transcription of an audio record	R20.00
	h) For a copy of an audio record	R30.00
3.	The request fee payable by a requester, other than a personal requester, referred to in regulation 11(2)	R50.00
4.	The request fee payable by a requester, other than a personal requester, referred to in regulation 11(3):	-
	a) For every photocopy of an A4 size page or part thereof	R1.10
	b) For a printed copy of an A4 size page or part thereof held on a computer or in electronic readable form	R0.75
	c) For a copy in a computer readable form on stiffy disc	R7.50
	d) For a copy in a computer readable form on compact disc	R70.00
	e) For a transcription of visual images, for an A4 size page or part thereof	R40.00
	f) For a copy of a visual image	R60.00
	g) For a transcription of an audio record, for A4 size page or part thereof	R20.00
	h) For a copy of an audio record	R30.00
5.	The actual postage fee is payable when a copy of a record must be posted to a requester	-
6.	For purposed of section 54(2) of the Act, the following applies:	-
	a) Six hours as the hours to be exceeded before a deposit is payable	-
	b) One third of the access fee is payable as a deposit by the requester	-