



REAL TIME TECHNOLOGIES
Registration Number: **2014/03/19**
"the Company"

Prepared in terms of section 51 of the Promotion of Access to Information Act, No. 2 of 2000, as amended.

Version 1.0
Date of compilation: x/x/2026

Table of Contents

1	Definitions.....	3
2	Purpose of the PAIA Manual	3
3	Contact Details for Access to Information Requests.....	4
4	Guide on how to use PAIA and how to Obtain Access to the Guide	4
5	Latest Notices in terms of Section 52(2) of PAIA	5
6	Availability of Certain Records in terms of PAIA	5
7	Request Process.....	10
8	Grounds for Refusal	12
9	Remedies Should a Request be Refused	13
10	Fees	13
11	Processing of Personal Information	14
12	The Recipients or Categories of Recipients to whom the Personal Information may be Supplied.....	14
13	Planned Transborder Flows of Personal Information.....	16
14	Availability of the PAIA Manual	16
15	Objection to the Processing of Personal Information by a Data Subject.....	16
16	Request for Correction/Deletion of Personal Information or Destruction/Deletion of Record of Personal Information	17
17	Applicable Forms	17
	PAIA Forms	Error! Bookmark not defined.
	Form 01: Request for a Copy of the Guide from an Information Officer [Regulation 3]	Error! Bookmark not defined.
	Form 02: Request for Access to Record [Regulation 7].....	Error! Bookmark not defined.
	Form 03: Outcome of Request and of Fees Payable [Regulation 8]	Error! Bookmark not defined.
	Form 05: Complaint Form [Regulation 10]	Error! Bookmark not defined.
	Form 13: PAIA Request for Compliance Assessment Form [Regulation 14(1)].	Error! Bookmark not defined.
	POPIA Forms	Error! Bookmark not defined.
	Form 1: Objection to the Processing of Personal Information	Error! Bookmark not defined.
	Form 2: Request for Correction of Deletion of Personal Information or Deletion of Record of Personal Information.....	Error! Bookmark not defined.
	Form 3: Application for the Issue of a Code of Conduct	Error! Bookmark not defined.
	Form 4: Application for the Consent of a Data Subject for the Processing of Personal Information for the Purpose of Direct Marketing	Error! Bookmark not defined.
	Form 5: Complaint Regarding Interference with the Protection of Personal Information for the Purpose of Direct Marketing.....	Error! Bookmark not defined.
18	Updating of the Manual.....	17

1 Definitions

Term	Definition
CEO	Chief Executive Officer
Client	Any natural or juristic person that received or receives services from the company
Complainant	Any person who lodges a complaint with the Information Regulator
Complaint	(a) A matter reported to the Information Regulator in terms of section 74(1) and (2) of the Act; (b) A complaint referred to in section 76(1)(e) and 92(1) of the Act; (c) A matter reported or referred to the Information Regulator in terms of other legislation that regulates the mandate of the Information Regulator
Conditions for Lawful Processing	The conditions for the lawful processing of personal information as fully set out in chapter 3 of POPI and in section 12 of this manual
Data Subject	The person to whom Personal Information relates
Day	A calendar day, unless the last day of a specified period happens to fall on a Sunday or public holiday, in which case it is calculated exclusive of that Sunday or public holiday (Interpretation Act, 1957 - Act No. 33 of 1957)
DIO	Deputy Information Officer
Information Officer/IO	The individual who is identified herein and legally appointed to ensure compliance with POPIA and PAIA
Manual	This manual
Minister	Minister of Justice and Correctional Services
Office Hours	(a) For the Information Regulator: 08:00–16:00, Monday to Friday (excluding public holidays); (b) For designated offices: Hours during which the offices operate
PAIA	The Promotion of Access to Information Act, No. 2 of 2000
Personal Information	Information relating to an identifiable living person, or an identifiable existing juristic person, including but not limited to race, gender, contact info, biometrics, correspondence, opinions, and identifiers
Personnel	Any person who works for or provides services to or on behalf of the company and receives or is entitled to receive remuneration, including permanent, temporary and part-time staff, directors, and contractors
POPI/POPIA	The Protection of Personal Information Act, No. 4 of 2013
POPI Regulations	Regulations promulgated in terms of section 112(2) of POPI
Private Body	(a) A natural person conducting business; (b) A business partnership; (c) A juristic person not being a public body
Processing	Any operation or activity concerning personal information, including collection, storage, dissemination, or destruction
Regulator	Information Regulator established in terms of POPIA
Republic	Republic of South Africa
Signature	Any legally accepted form of signature, including electronic signature where applicable
Writing	As referred to in section 12 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)

2 Purpose of the PAIA Manual

Commented [NM1]: A PAIA Manual outlines the records held by a company and the process for requesting access to such information.

This PAIA Manual is useful for the public to:

- 2.1 The PAIA Manual serves as a public guide to the information held by the organisation and how it can be accessed. It outlines the categories of records available without a formal request, the subjects on which records are maintained, and details of records accessible under other legislation. The manual also provides the official contact details of the Information Officer (IO) and Deputy Information Officer (DIO), who are responsible for assisting the public in exercising their right of access.
- 2.2 The manual further explains how to use the PAIA process and where to obtain the official guide published by the Regulator. It describes whether and how the organisation processes personal information, including the purposes of processing, the categories of data subjects involved, and the recipients (local or international) to whom such information may be supplied. The manual further confirms that appropriate security safeguards are in place to protect the confidentiality, integrity, and availability of personal information.

3 Contact Details for Access to Information Requests

3.1 Information Officer

Name	Michael Vermeulen
Contact number	083 353 7333
Email address	michael@realtime-technologies.com / Info@realtime-technologies.com

3.2 Deputy Information Officer

Name	Christina Vermeulen
Contact number	010 593 0999
Email address	Tania@realtime-technologies.com

3.3 National or head office

Postal address	62A Norite Road, Helderkruijn, Roodepoort, Gauteng, 1724
Physical address	62A Norite Road, Helderkruijn, Roodepoort, Gauteng, 1724
Contact number	010 593 0999
Email	Info@realtime-technologies.com
Website	https://www.realtime-technologies.com/

4 Guide on how to use PAIA and how to Obtain Access to the Guide

- 4.1 The Information Regulator has published a revised PAIA Guide in terms of section 10(1) of PAIA (as amended). This guide is designed to help any person who wishes to exercise rights under PAIA or POPIA, and it is available in all official languages as well as in braille to ensure accessibility.
- 4.2 The Guide serves two key purposes:
 - 4.2.1. Access to Personal Information (POPIA): It explains how individuals (data subjects) can exercise their rights to request confirmation of whether personal information is held about them, to access that information (including details of third-party recipients), and to request correction, deletion, or destruction of personal information that is inaccurate, outdated, excessive, or unlawfully obtained.

Commented [NM2]: Speaks to the guidance notes published by the information regulator

- 4.2.2. Access to Records (PAIA): It provides step-by-step guidance on how to request records from public or private bodies, including the required forms, the process for appeals or complaints, and how to approach a court if necessary.

4.3 In addition, the Guide offers:

- 4.3.1. An overview of the objectives of PAIA and POPIA.
 4.3.2. Contact details of Information Officers (IOs) and Deputy Information Officers (DIOs).¹
 4.3.3. Manner and form of a request for access to a record of a public body and private body.²
 4.3.4. Guidance on compiling or accessing PAIA Manuals.³
 4.3.5. Information on voluntary disclosures of records, prescribed access fees, and applicable regulations.⁴
 4.3.1.1 How to lodge an internal appeal, a complaint with the Regulator or apply to court for a against a decision by the IO of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body.

- 4.3.6. Insight into how PAIA has been amended following the implementation of POPIA.

4.4 The guide can also be obtained:

- 4.4.1 Upon request to the IO: [Request for a Copy of the Guide from an Information Officer \[Regulation 3\]](#)
 4.4.2 From the website of the Regulator: www.inforegulator.org.za
 4.4.3 From the offices of the Regulator: Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg OR by email: enquiries@inforegulator.org.za

4.5 A copy of the guide is also available in the following three official languages, for public inspection during normal office hours:

- 4.5.1 English.
 4.5.2 Afrikaans.
 4.5.3 Zulu.

5 Latest Notices in terms of Section 52(2) of PAIA

At this stage, no notice(s) has/have been published on the categories of records that are available without having to request access to them in terms of PAIA.

6 Availability of Certain Records in terms of PAIA

6.1 Categories of records of the company which are available without a person having to request access:

Category of Records	Types of the Record	Available on Website	Available on Request
PAIA Manual	Current PAIA Manual, version and effective date	X	X

Commented [NM3]: This section explains which records are automatically available to the public without a formal request, and how they can be accessed.

¹ Section 56(a) of POPIA - Every public and private body must, in line with section 17 of PAIA, appoint as many Deputy Information Officers as needed to carry out the duties and responsibilities set out in section 55(1) of POPIA.

² In terms of PAIA, access to records of a public body (section 11) or a private body (section 50) must be granted if the requester meets PAIA's procedural requirements, the request is necessary for exercising or protecting a right (in the case of private bodies), and no grounds for refusal in Chapter 4 apply.

³ In terms of sections 14 and 51 of PAIA, the Information Officer of every public and private body must update and publish their PAIA manual at least once every 12 months.

⁴ In terms of PAIA, public and private bodies must keep their PAIA manuals (sections 14 and 51) and notices (sections 15 and 52) updated and published at least once every 12 months. When access to a record is granted, the notice must also state any access fee payable by the requester (sections 22 and 54). In addition, the Information Regulator must update and publish the official PAIA Guide at least once every two years (section 92(1)).

Category of Records	Types of the Record	Available on Website	Available on Request
Company overview	Company profile, telecommunications and cloud service offerings, sectors served, head office contact details	X	X
Services and capabilities	CCTV surveillance solutions (Hikvision, Dahua, UNV), VoIP solutions, Hosted PABX, Cloud-based switchboard systems, PCI-compliant call recording, network infrastructure (Cat5/Cat6), firewall and wireless solutions, solar	X	X
Technology partners & platforms	High-level list of CCTV brands (e.g., Hikvision, Dahua, UNV) and telecommunications/cloud platforms implemented (excluding client-specific configurations)	X	X
CCTV Service Information	General system capabilities and surveillance solution descriptions (excluding client footage, site layouts, or monitoring data)	-	X
Voice and Telecommunications Solutions	Hosted PABX features, VoIP configurations, call routing systems, extension management, auto-attendant functionality (excluding client-specific system settings)	-	X
Cloud Hosting and Redundancy Framework	High-level description of cloud-based infrastructure and redundancy measures ensuring business continuity	X	X
PCI-Compliant Call Recording Framework	General compliance approach to secure call recording and cardholder data protection (excluding recorded calls or security configurations)	-	X
Network Infrastructure Documentation	Installation standards, cabling specifications (Cat5/Cat6), optimisation practices (excluding site-specific diagrams)	-	X
Cybersecurity and Firewall Services	Firewall implementation approach, risk assessment methodology (excluding credentials and security architecture details)	-	X
Installation and Handover Documentation	Site sign-off documentation and implementation summaries (client-specific documentation not publicly available)	-	X
Policies public facing	Privacy and Cookie Policy, Website Terms	X	X
Legal disclosures	POPIA and PAIA statements, website disclaimers	X	X
Public marketing materials	Brochures, capability decks, gallery images without site identifiers	X	X
Health and safety documentation	Health and Safety Policy and site installation safety procedures	X	X
Tender or supplier onboarding info	Vendor onboarding forms, B-BBEE certificate/affidavit, bank confirmation letter (where applicable)	X	X

Category of Records	Types of the Record	Available on Website	Available on Request
Corporate Identifiers	Registered name, registration number, registered address, VAT number	-	X
Information Officer contacts	Information Officer and any Delegated IO names, roles, email addresses, contact numbers	X	X
IO registration proof	Information Regulator registration certificate or reference number	-	X
Company secretarial snapshot	Directors' names as filed at CIPC, principal place of business	-	X
Tax and compliance attestations	SARS TCS PIN, COID Letter of Good Standing, UIF confirmation	-	X
Insurance confirmations	Public liability insurance confirmation, limits, validity dates	-	X
Supplier Code of Conduct	Ethics, anti bribery, gifts and hospitality, conflicts of interest	-	X
Standard procurement info	Supplier onboarding requirements and payment terms summary	X	X

6.2 Description of the records/subjects of the company which are available in accordance with any other legislation:

Category of Records	Applicable Legislation
Memorandum of Incorporation, CIPC filings	Companies Act, 2008. Act 71 of 2008
Beneficial ownership register, filings, access log	Companies Regulations, 2011 as amended by Companies Amendment Regulations on Beneficial Ownership, 2023
Director and prescribed officer disclosures, conflict registers, resolutions	Companies Act, 2008. Act 71 of 2008
Employment contracts, attendance, overtime, payroll, leave	Basic Conditions of Employment Act, 1997. Act 75 of 1997
National Minimum Wage schedules for technicians and field teams	National Minimum Wage Act, 2018. Act 9 of 2018 read with the Basic Conditions of Employment Act, 1997
Disciplinary and grievance files, union correspondence, CCMA files	Labour Relations Act, 1995. Act 66 of 1995
Employment Equity plan, annual EE reports, committee minutes	Employment Equity Act, 1998. Act 55 of 1998
Recruitment ads, shortlist records, background screening outcomes	Employment Services Act, 2014. Act 4 of 2014. Protection of Personal Information Act, 2013. Act 4 of 2013

Category of Records	Applicable Legislation
Work permission for foreign nationals	Immigration Act, 2002. Act 13 of 2002
UIF declarations, contribution records, benefit claims	Unemployment Insurance Act, 2001. Act 63 of 2001
Skills plans, annual training reports, learnership agreements	Skills Development Act, 1998. Act 97 of 1998
Levy declarations, SETA registrations, grants	Skills Development Levies Act, 1999. Act 9 of 1999
PAYE, IRP5, EMP201, EMP501, tax directives	Income Tax Act, 1962. Act 58 of 1962
VAT returns, input and output schedules, SARS correspondence	Value Added Tax Act, 1991. Act 89 of 1991
COIDA registration, Return of Earnings, Letter of Good Standing, IOD claims	Compensation for Occupational Injuries and Diseases Act, 1993. Act 130 of 1993
OHS policy, site risk assessments, incident reports, safety minutes	Occupational Health and Safety Act, 1993. Act 85 of 1993 and regulations including Construction Regulations, Electrical Machinery Regulations
Public liability policy schedules, endorsements, notifications	Insurance Act, 2017. Act 18 of 2017
B-BBEE certificate, ownership, skills, supplier and enterprise development evidence	Broad Based Black Economic Empowerment Act, 2003. Act 53 of 2003 and the Codes of Good Practice
Client service agreements (CCTV, VoIP, PABX, network installations)	Consumer Protection Act, 2008. Act 68 of 2008
Telecommunications service agreements and voice provider contracts	Electronic Communications Act, 2005 (Act 36 of 2005)
ICASA-related licences or service compliance (where applicable)	Electronic Communications Act, 2005 & ICASA Regulations
Hosted PABX and VoIP system documentation	Electronic Communications and Transactions Act, 2002

Category of Records	Applicable Legislation
PCI-compliant call recording framework	POPIA & applicable PCI-DSS Standards
Call recording consents and interception documentation	Regulation of Interception of Communications Act, 2002 (RICA)
Data subject notices, consent records, operator agreements, retention schedules	Protection of Personal Information Act, 2013. Act 4 of 2013
Data retention schedules (CCTV footage, call recordings)	Protection of Personal Information Act, 2013. Act 4 of 2013
Security policies, access controls, breach register, Regulator and data subject notifications	POPIA sections 19 to 22
Information Regulator correspondence, remedial actions evidence	POPIA sections 22 to 23
Data subject rights register, outcomes, response packs	POPIA sections 23 to 25
Cross border transfer assessments and safeguards for cloud hosting	POPIA section 72
DIO designations and revocations, IO registration proof	POPIA Regulations and outputs from the Information Regulator portal
PAIA Manual, access request log, decision register, fee records, training logs	Promotion of Access to Information Act, 2000. Act 2 of 2000
Electronic communications policies, e signature consents, website terms	Electronic Communications and Transactions Act, 2002. Act 25 of 2002
Call recording policies, interception consents for support or QA	Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002. Act 70 of 2002
Cyber incident register, takedown requests, forensic reports	Cybercrimes Act, 2020. Act 19 of 2020
Firewall configurations and cybersecurity controls	POPIA & Cybercrimes Act, 2020

Category of Records	Applicable Legislation
Network infrastructure documentation (Cat5/Cat6 installations)	OHS Act & contractual obligations
CCTV system documentation and footage	POPIA
Fleet records (installation vehicles, driver licences)	National Road Traffic Act, 1996
CCTV footage at office or stores. Visitor registers	POPIA. Private Security Industry Regulation Act, 2001. Act 56 of 2001
Site access permits, contractor permits	OHS Act, 1993 and client site rules via contract
Pressure equipment, lifting equipment and tools inspection files where used	OHS Act Pressure Equipment Regulations and Driven Machinery Regulations
Gifts and hospitality registers, conflict of interest logs, third party risk	Prevention and Combating of Corrupt Activities Act, 2004. Act 12 of 2004
Email retention rules, journaling settings, legal hold notices	POPIA and applicable Rules of Court on discovery and preservation

- 6.3 The company keeps certain records as required by PAIA and POPIA:
- 6.3.1 PAIA records: PAIA Manual, official guides, submission records, and awareness training materials.
- 6.3.2 POPIA records: Information Officer registration certificate, data breach records, retention records, and awareness training materials.
- 6.3.3 Other relevant information may also be made available on request.
- 6.4 The tabulated records may be requested; however, it should be noted that there is no guarantee that the request will be honoured. Each request will be evaluated in terms of PAIA and any other applicable legislation.

7 Request Process

An individual who wishes to place a request must comply with all the procedures laid down in PAIA:

7.1. Initiating the request

- 7.1.1. Use the prescribed form
- All requests must be made on the prescribed form (**Form 2 – Request for Access to Record [Regulation 7]**) - [Request for Access to Record \[Regulation 7\]](#)
 - Additional prescribed forms include:
 - **Form 2 – Request for Correction or Deletion** (section 24 of POPIA). This form is used by a data subject to request the correction of inaccurate, outdated, incomplete, irrelevant, or misleading personal information, and/or the deletion or destruction of

personal information that is no longer necessary or unlawfully obtained, in accordance with Section 24(1) of POPIA. It ensures that responsible parties maintain accurate and lawful records of personal data. - [Request for Correction or Deletion of Personal Information or Deletion of Record of Personal Information](#)

- **Form 3 – Application for a Code of Conduct** (section 61 of POPIA). This form is used by an industry body, profession, or class of entities to apply for the issuance of a Code of Conduct under Section 61(1)(b) of POPIA. It allows industries to self-regulate how personal information is processed within their sector, in line with the conditions for lawful processing. - [Application for the Issue of a Code of Conduct](#)
- **Form 4 – Request for Consent for Direct Marketing** (section 69 of POPIA). This form enables a responsible party to formally request a data subject's consent to receive direct marketing communications via unsolicited electronic means (e.g., SMS, email), as required under Section 69(2) of POPIA. It ensures that individuals have control over whether and how they are marketed to. - [Application for the Consent of a Data Subject for the Processing of Personal Information for the Purpose of Direct Marketing](#)
- **Form 5 – Complaint Regarding Interference with Personal Information**. This form (Information) allows a data subject or complainant to submit a complaint to the Regulator concerning unlawful interference with personal information; or a determination made by an adjudicator under POPIA. It provides an avenue for recourse and investigation in cases of non-compliance with data protection obligations. - [Complaint Regarding Interference with the Protection of Personal Information for the Purpose of Direct Marketing](#)

7.1.2. Requests not submitted on the prescribed form may be rejected.

7.1.3. Assistance in the request process:

- If a requester is illiterate or disabled, they may make the request orally to the IO, who must complete the prescribed form on their behalf and provide them with a copy (section 18(3) of PAIA).
- The IO must provide reasonable assistance to any requester who requires help in completing the form or understanding the procedure.

7.2. Particulars of the Request

7.2.1. The request must provide sufficient detail to enable the IO to identify and process it. This includes:

- A clear description of the record(s) requested.
- Full identity of the requester, with proof of identity where required.
- The preferred form of access (inspection, copy, electronic copy, etc.).
- The requester's contact details (postal, physical, fax or email).
- A statement that the record is required to exercise or protect a right, specifying the nature of that right and explaining why the record is necessary.
- If a request is made on behalf of another person, proof of authorisation must be attached.

7.3. Submission of Requests

7.3.1. The completed form, together with proof of payment of the prescribed request fee (if applicable), must be submitted to the Information Officer (IO) at the Company.

7.3.2. Requests may be lodged by:

- Hand delivery to the physical address provided in this Manual;
- Postal delivery to the Company's registered address;
- Fax; or
- Email to the address of the IO or DIO.

- 7.3.3. Where applicable, the IO may require a deposit in terms of section 22(2) of PAIA where search and preparation is expected to be time-consuming.

7.4. Fees and Timeframes for Response

- 7.4.1. Requests will be processed and responded to within 30 (thirty) calendar days of receipt.
- 7.4.2. In terms of section 26 of PAIA, the IO may extend this period once, by up to 30 additional days, if:
- The request involves a large number of records;
 - Consultation with third parties is required; or
 - The records are located in another office and cannot reasonably be obtained within 30 days.
- 7.4.3. If an extension is required, the requester will be notified in writing, with reasons for the extension.
- 7.4.4. A request fee may be charged for non-personal requests.
- 7.4.5. If the search and preparation of the record will exceed six (6) hours, the requester may be required to pay a deposit of up to one-third of the estimated fee.
- 7.4.6. Access will only be granted once all required fees have been paid.

7.5. Outcome of Request

- 7.5.1. The IO will notify the requester in writing, using **Form 3 - Outcome of Request and of Fees Payable** [Regulation 8], of the decision to grant or refuse access.
- 7.5.2. If access is granted, the notice will:
- Specify the form of access; and
 - State the applicable access fees payable before access is given.
- 7.5.3. If access is refused, the notice will set out the grounds for refusal as provided in Chapter 4 of PAIA.

7.6. Appeals and Complaints

- 7.6.1. If access is refused or deemed refused (i.e. no decision within the prescribed period), the requester may:
- Lodge an internal appeal (for public bodies); or
 - Refer the matter to the Information Regulator or approach a court of law (for private bodies).
- 7.6.2. The Regulator can be contacted using the details provided in this Manual.

8 Grounds for Refusal

In terms of Chapter 4 of PAIA, the company may refuse a request for access to records on the following grounds (unless an exception applies):

- 8.1 **Privacy of individuals** - To protect the personal information of a third party (including deceased persons) where disclosure would be unreasonable.
- 8.2 **Commercial interests of third parties** - Records may be refused if they contain:
- Trade secrets;
 - Financial, commercial, scientific, or technical information, where disclosure could cause harm; or
 - Information provided in confidence, where disclosure could disadvantage or prejudice the third party in negotiations or competition.
- 8.3 **Confidentiality agreements** - Information that is protected under a contract or agreement with a third party.
- 8.4 **Safety and security** - Records that could endanger the life, health, or safety of a person, or the protection of property.
- 8.5 **Legal privilege** - Records that would be privileged from disclosure in legal proceedings.

- 8.6 **Commercial interests of the company** - Records may be refused if they contain:
- Trade secrets;
 - Financial, commercial, scientific, or technical information that could harm the company's interests;
 - Information that could prejudice the company in negotiations or competition; or
 - Proprietary computer programs protected by copyright or intellectual property law.
- 8.7 **Research information** - Where disclosure would place ongoing research or a researcher at a serious disadvantage.
- 8.8 **Frivolous or unreasonable requests** - Requests that are clearly frivolous, vexatious, or that would cause an unreasonable burden on company resources.

9 Remedies Should a Request be Refused

- 9.1 If the company does not have an internal appeal procedure in light of a denial of a request, decisions made by the IO is final.
- 9.2 The requestor may in accordance with sections 56(3) (c) and 78 of PAIA, apply to a court for relief within 180 (one-hundred-and-eighty) days of notification of the decision for appropriate relief.

10 Fees

The following fees shall be payable upon request by a requestor:

Details	Fee
Request fee (payable on every request)	R140.00 once-off
Photocopy of an A4 page or part thereof	R2.00 per page
Printed copy of an A4 page or part thereof	R2.00 per page
Hard copy on flash drive (flash drive to be provided by requestor)	R40.00 once-off
Hard copy on a compact disc (compact disc to be provided by requestor)	R40.00 once-off
Hard copy on a compact disc (compact disc to be provided by the company)	R60.00 once-off
Transcription of visual images per A4 page	As per quotation of service provider
Copy of visual images	As per quotation of service provider
Transcription of an audio record	R24.00 per A4 page
Copy of an audio record on flash drive (flash drive to be provided by requestor)	R40.00 once-off
Copy of an audio on a compact disc (compact disc to be provided by requestor)	R40.00 once-off
Copy of an audio on a compact disc (compact disc to be provided by the company)	R60.00 once-off
Base/starting rate to search for and prepare the record for disclosure	R145.00 per hour for each hour or part thereof, excluding the first hour, reasonably required for such search and preparation (cannot exceed R435.00 per request)
Rate to search for and prepare the record for disclosure	R435.00 per hour for each hour or part thereof, excluding the first hour, reasonably required for such search and preparation (cannot exceed total cost)
Postage, email or any other electronic transfer	Actual expense, if any

Commented [NM4]: When a person requests access to records, the organisation may need to search for the record (e.g., in archives, systems, or paper files) and prepare it for disclosure (e.g., collating, redacting personal/confidential info, copying).
The first hour of work is free.
After the first hour, the requester is charged a fee per additional hour (or part thereof).

Commented [NM5]: Max amount

11 Processing of Personal Information

11.1 The company processes personal information in accordance with the conditions for lawful processing as set out in the Protection of Personal Information Act, 4 of 2013 (“POPIA”). Personal information is processed only for legitimate business purposes, which may include (but are not limited to):

- 11.1.1 Employment-related purposes: Recruitment, administration of employment contracts, payroll, benefits, training, and compliance with labour laws.
- 11.1.2 Client and supplier management: Entering into and performing contracts, maintaining relationships, processing payments, and responding to queries or complaints.
- 11.1.3 Legal and compliance obligations: Compliance with statutory and regulatory requirements, record keeping, audits, and reporting.
- 11.1.4 Security and risk management: Protecting company property, monitoring access, preventing fraud, and ensuring the safety of staff, clients, and visitors.
- 11.1.5 Marketing and communication: Providing information about products or services, subject to obtaining the necessary consent under POPIA.

11.2 The company ensures that personal information is processed lawfully, reasonably, and only for the purposes for which it was collected and takes appropriate steps to protect the confidentiality and integrity of such information.

11.3 Description of the categories of data subjects and of the information or categories of information relating thereto:

11.3.1. The company processes personal information relating to various categories of data subjects. The categories of data subjects, and the types of personal information that may be processed in respect of each, include (but are not limited to) the following:

Categories of Data Subjects	Personal Information that may be Processed
Corporate Clients (Telecommunications, CCTV, VoIP, PABX customers)	Names, job titles, business contact details, company registration details, VAT numbers, contract documentation, service level agreements, quotations, invoices, payment history, bank confirmation letters, support tickets, call logs metadata, installation records, correspondence.
Residential CCTV Clients (Home Surveillance Customers)	Full names, contact details, installation addresses, ID numbers where required for contracting, payment records, service history, CCTV footage captured at client premises (as operator where applicable), maintenance logs, technical configuration data.
End Users of Client Systems (Callers to Hosted PABX / Recorded Lines)	Voice recordings (where call recording is enabled and lawful), call metadata (date, time, duration), extension numbers, call routing information. Cardholder data is not stored where PCI-compliant solutions are implemented..
Voice and Telecommunications Users (VoIP / Hosted PABX extensions)	Names, extension numbers, internal contact details, usage logs, voicemail records (where enabled), device identifiers, system access logs.
Cloud Hosting Clients	Account details, service configurations, system credentials (encrypted), uptime and redundancy logs, support interactions, billing records.
Technology and Equipment Suppliers (CCTV, VoIP, networking hardware)	Company details, registration and VAT numbers, B-BBEE status, bank details, contact persons, quotations, purchase orders, warranties, SLAs, compliance declarations, security questionnaires, operator agreements.

Commented [NM6]: This section describes the different types of data subjects (e.g., customers, employees, suppliers) and the personal information collected, processed, and stored about each category.

Subcontractors and specialist installers	Company and contact details, scope of work, competency records, permits to work, induction and safety confirmations, incident logs, invoices, communications.
Employees	Names, identity numbers, contact details, demographic data (for Employment Equity reporting), next of kin, employment contracts, payroll and tax information, benefits data, performance records, disciplinary records, training completion, device assignments, access control logs, email and system usage logs, health and safety records where applicable.
Field technicians and site engineers	Names, contact details, job schedules, device identifiers, GPS logs (where enabled), job card uploads, installation photographs, site access permits, overtime records, competency certificates, driver licence details (if applicable).
Drivers(Company Vehicles)	Names, licence and PDP details, vehicle allocation records, telematics and GPS logs, fuel usage logs, accident and incident reports, infringement notices.
Job applicants	Names, contact details, CVs, qualifications, work history, references, background screening outcomes, right to work records, interview notes.
Website users and online portal users	Names and contact details submitted via online forms, IP addresses, browser/device identifiers, cookies, analytics data, timestamps, enquiry content.
Office and workshop visitors. CCTV subjects	Names, ID or visitor card details, access logs, CCTV images and video, vehicle registration for parking, contractor company details.
Shareholders, directors, prescribed officers	Names, identity numbers, contact details, shareholding details, appointments, CIPC filings, beneficial ownership particulars, conflict registers.
Regulators (Information Regulator, ICASA, SARS, Department of Labour, etc.)	Names, institutional roles, official contact details, correspondence records, inspection documentation, compliance submissions, licence references (where applicable).
Community stakeholders and complainants	Names, contact details, complaint or enquiry content, signatures for acknowledgements, related correspondence, the minimum content required for legal or operational response.

12 The Recipients or Categories of Recipients to whom the Personal Information may be Supplied

12.1 Personal information held by the company may be disseminated to third parties only when lawful and necessary for business, contractual, or regulatory purposes. Categories of personal information and possible recipients include (but are not limited to):

Category of Personal Information	Recipients or Categories of Recipients
Identity numbers, names, business and personal contact details	Government departments and regulators, law enforcement where required, auditors, banks for KYC, municipal authorities for site and vendor onboarding, logistics partners for equipment delivery, Information Regulator for statutory submissions.
Qualifications, licenses, and professional history	Professional bodies (e.g., ECSA for registered engineers), background screening providers, recruitment service providers, client audit teams under contractual obligations.
Credit and payment history	Registered credit bureaus. Banks and payment processors. External accountants. Debt collection agencies where applicable.
Tax and payroll records	SARS. Payroll providers. Pension or provident fund administrators. Medical aid and employee benefit providers. UIF and COID administrators.
Health and safety information	Occupational health practitioners. Medical aid providers. Workmen's Compensation authorities. Client site safety officers for incident escalation. Insurers and loss adjusters.

Commented [NM7]: This section explains who The company may share personal information with and under what circumstances, such as for legal compliance, business operations, or with the data subject's consent.

Contractual and business information	Clients, insurers, legal advisors, auditors, consultants, subcontractors, and technology partners under NDA, including distributors for warranty or service support.
B-BBEE credentials and supplier data	Verification agencies, client procurement teams, tender portals where disclosure is required.
Training and induction records	Client site induction portals, auditors.
Direct marketing preferences and contact data	Email and SMS service providers. Campaign management vendors. Suppression list partners to honor opt outs.
Project acceptance, commissioning, FAT SAT records	Clients, independent certifiers or engineers where required, regulators only if submission is legally required.
CCTV footage, access control logs, visitor registers	Security service providers, landlords/centers for shared premises, insurers, law enforcement on request, forensic investigators.
Financial records, invoices, bank details	Banks. External accountants. Auditors. Payment processors. Clients and suppliers for reconciliation.
Digital and IT records including user IDs, device IDs, logs	Cloud hosting providers. Managed IT and cybersecurity vendors. SaaS analytics providers. Incident response partners.
Network and telecom configuration snapshots with access metadata	Client technical teams, managed service providers for break/fix or upgrades. Never shared publicly.
Data protection governance records including ROPA, operator agreements, breach logs	Information Regulator. Clients in their capacity as responsible parties. Legal counsel. Insurers for cyber coverage.
Procurement and vendor onboarding packs	Due diligence providers, screening databases, client procurement teams, group legal and risk.
Shareholder, director, and beneficial ownership details	CIPC. Banks for KYC. Auditors. Verification agencies where tender rules require disclosure.

13 Planned Transborder Flows of Personal Information

- 13.1 The company may, where necessary and lawful, transfer or store personal information outside the Republic of South Africa. This could include, for example, the use of secure cloud-based service providers or international business partners. Where no transborder transfer is required, personal information will continue to be stored and processed within South Africa.
- 13.2 Any cross-border transfer of personal information will only take place in accordance with section 72 of POPIA, which requires that:
- 13.2.1 The recipient country, organisation, or international organisation is subject to a law, binding agreement, or corporate rules that provide an adequate level of protection; or
- 13.2.2 The transfer is necessary for the performance of a contract, with the consent of the data subject, or for another lawful reason recognised by POPIA.

14 Availability of the PAIA Manual at the Company

- 14.1 A copy of the manual is available:
- 14.1.1 On the website or at any head office for public inspection during normal business hours;
- 14.1.2 To any person upon request and upon the payment of a reasonable prescribed fee; and
- 14.1.3 To the Information Regulator upon request.
- 14.2 A fee for a copy of the manual, as contemplated in the Regulations, shall be payable per each A4-size photocopy made.

15 Objection to the Processing of Personal Information by a Data Subject

- 15.1 Any person (“data subject”) has the right to object to the processing of their personal information in terms of section 11(3) of POPIA.
- 15.2 An objection must be made on **Form 1 – [Objection to the Processing of Personal Information](#)** or a similar form. This is free of charge and can be sent by hand, post, fax, email, SMS, WhatsApp, or any other convenient method.
- 15.3 When personal information is collected, the company must inform the data subject of their right to object.
- 15.4 If an objection is made by phone, the company must record it electronically and provide a copy or written transcript to the data subject on request, at no cost.

16 Request for Correction/Deletion of Personal Information or Destruction/Deletion of Record of Personal Information

- 16.1 A data subject has the right, under section 24 of POPIA, to request the correction, destruction, or deletion of their personal information at any time and free of charge.
- 16.2 Correction or deletion may be requested if the personal information is:
- 16.2.1 Inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or unlawfully obtained;
or
- 16.2.2 No longer lawfully permitted to be kept by the company.
- 16.3 Requests must be made using **Form 2 – [Request for Correction of Deletion of Personal Information or Deletion of Record of Personal Information](#)** or a similar form. This can be submitted free of charge by hand, post, fax, email, SMS, WhatsApp, or any other convenient method.
- 16.4 If a request is made by phone, the company must record it electronically and provide a copy or written transcript to the data subject on request, at no cost.
- 16.5 The company must respond within 30 days of receiving the request and notify the data subject in writing of the outcome and any action taken.

17 Applicable Forms

PAIA Forms

- Form 01:** [Request for a Copy of the Guide from an Information Officer \[Regulation 3\]](#)
- Form 02:** [Request for Access to Record \[Regulation 7\]](#)
- Form 03:** [Outcome of Request and of Fees Payable \[Regulation 8\]](#)
- Form 05:** [Complaint Form \[Regulation 10\]](#)
- Form 13:** [PAIA Request for Compliance Assessment Form \[Regulation 14\(1\)\]](#)

POPIA Forms

- Form 1:** [Objection to the Processing of Personal Information](#)
- Form 2:** [Request for Correction of Deletion of Personal Information or Deletion of Record of Personal Information](#)
- Form 3:** [Application for the Issue of a Code of Conduct](#)
- Form 4:** [Application for the Consent of a Data Subject for the Processing of Personal Information for the Purpose of Direct Marketing](#)
- Form 5:** [Complaint Regarding Interference with the Protection of Personal Information for the Purpose of Direct Marketing](#)

18 Updating of the Manual

The head of the company will update this manual on a regular basis.

Commented [NM8]: Form 01-Request for a copy of the guide

Commented [NM9]: Form 02- Request for access to the record.

Commented [NM10]: Outcome of Request and of Fees Payable [Regulation 8]
Completed by the Information Officer to inform the requester whether access has been granted or refused, and the applicable fees.

Commented [NM11]: Complaint Form [Regulation 10]
Used by a requester to lodge a complaint with the Information Regulator about how their PAIA request was handled

Commented [NM12]: PAIA Request for Compliance Assessment Form [Regulation 14(1)]
Submitted to the Information Regulator when a requester wishes the Regulator to assess whether the organisation has complied with PAIA obligations.

Commented [NM13]: Purpose of Form 3:
This form is used by industry associations or bodies (not individual data subjects) to apply to the Information Regulator for approval of a Code of Conduct. A Code of Conduct sets out how members of a specific industry or sector will handle personal information in line with **POPIA**. Once approved by the Regulator, it provides guidance and standards for compliant processing of personal information within that sector.

Commented [NM14]: Used where consent is required to process personal information for direct marketing purposes (e.g., promotional emails or SMS)

Commented [NM15]: Used when a data subject wishes to complain to the Information Regulator about unwanted or unlawful direct marketing practices.

Name of IO	Michael Vermeulen
Title of the head of the body	Director