



PAIA MANUAL

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 in respect of the South African entities of Vantage Data Centers, as listed in section 3 of this Manual, each a private body (the “Vantage Entities”).

Document Owner		Additional Reviewers	
Information Officer		Corporate Compliance	
Filename		Version	Date Published
VDC – PAIA Manual		1.0	02/11/2026

Table of Contents

1	LIST OF ACRONYMS AND ABBREVIATIONS	3
2	PURPOSE OF PAIA MANUAL	3
3	APPLICABLE ENTITIES	4
4	KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF THE VANTAGE ENTITIES	4
5	GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE	5
6	CATEGORIES OF RECORDS WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS	6
7	DESCRIPTION OF THE RECORDS AND RECORD CATEGORIES WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION	6
8	PROCESSING OF PERSONAL INFORMATION	8
9	AVAILABILITY OF THE MANUAL	14
10	PROCEDURE FOR REQUESTING ACCESS TO INFORMATION IN TERMS OF PAIA	14
11	DOCUMENT CONTROL	15
	REVISION HISTORY	15
	ANNUAL REVIEW	16

1 LIST OF ACRONYMS AND ABBREVIATIONS

- “CEO” means “Chief Executive Officer”;
- “DIO” means “Deputy Information Officer”;
- “IO” means “Information Officer”;
- “Minister” means “Minister of Justice and Correctional Services”;
- “PAIA” means “Promotion of Access to Information Act No. 2 of 2000 as amended and any regulations, codes of conduct, directives, rulings, orders or guidelines published thereunder and/or by the Regulator, from time to time”;
- “POPIA” means “Protection of Personal Information Act No. 4 of 2013 as amended and any regulations, codes of conduct, directives, rulings, orders or guidelines published thereunder and/or by the Regulator, from time to time”;
- “Regulator” means “Information Regulator as established in terms of POPIA”; and
- “South Africa” means “Republic of South Africa”

2 PURPOSE OF PAIA MANUAL

This Manual has been prepared in accordance with section 51 of PAIA, as read with POPIA, in respect of the Vantage Entities. This Manual facilitates requests for access to records of the Vantage Entities and is useful for the public to:

- check the categories of records held by the Vantage Entities which are available without a person having to submit a formal PAIA request;
- have a sufficient understanding of how to make a request for access to a record of the Vantage Entities, by providing a description of the subjects on which the Vantage Entities hold records and the categories of records held on each subject;
- know the description of the records of the Vantage Entities which are available in accordance with any other legislation;
- access all the relevant contact details of the IO and DIO who will assist the public with the records they intend to access;
- know the description of the guide on how to use PAIA, as updated by the Regulator from time to time, and how to obtain access to it;
- know if the Vantage Entities will process personal information, and the purpose for processing of such personal information;
- know the description of the categories of subjects and of the information or categories of information relating to such subjects;
- know the recipients or categories of recipients to whom the personal information may be supplied by any and/or all of the Vantage Entities;
- know if the Vantage Entities have planned to transfer or process personal information outside South Africa; and

- know whether the Vantage Entities have appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3 APPLICABLE ENTITIES

This Manual has been prepared in respect of the following entities:

Corporate name	Registered office	Registration number
VDC CPT11 (PTY) LTD	Merlot House, The Vineyards Office Estate, 99 Jip De Jager Drive, Bellville, Western Cape, South Africa, 7530	2020/851531/07
VDC JNB11 OPCO (PTY) LTD		2020/851514/07
VDC JNB11 PROPCO (PTY) LTD		2020/851485/07
VDC JNB12 PROPCO (PTY) LTD		2022/759295/07
VDC JNB12 OPCO (PTY) LTD		2023/518144/07
VDC SOUTH AFRICA OPCO (PTY) LTD		2023/514600/07
VDC JNB13 PROPCO (PTY) LTD		2023/887601/07

The Manual is limited to the records held by the abovementioned Vantage Entities in respect of their operations.

4 KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF THE VANTAGE ENTITIES

Information Officer

Name: Andy Jones

Tel: 07943373687

Email: a.jones@vantage-dc.com

Deputy Information Officer

Name: Richard Collinson

Tel: 07483179553

Email: Privacy.Office@Vantage-dc.com

National or Head Office

Physical and Postal Address: Merlot House, The Vineyards Office Estate, 99 Jip De Jager Drive, Bellville, Western Cape, South Africa, 7530

Telephone: +44 (0) 1633 988 021

Website: <https://vantage-dc.com/>

5 GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

The Regulator has, in terms of section 10(1) of PAIA, updated and made available the revised guide on how to use PAIA (“**Guide**”), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA. The aforesaid Guide contains the description of:

- the objects of PAIA and POPIA;
- the postal and street address, phone and fax number and, if available, electronic mail address of:
 - the IO of every public body, and
 - every DIO of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA;
- the manner and form of a request for:
 - access to a record of a public body contemplated in section 11 of PAIA; and
 - access to a record of a private body contemplated in section 50 of PAIA;
- the assistance available from the IO of a public body in terms of PAIA and POPIA;
- the assistance available from the Regulator in terms of PAIA and POPIA;
- all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging:
 - an internal appeal;
 - a complaint to the Regulator; and
 - an application with a court 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;
- the provisions of sections 14 and 51 of PAIA requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
- the provisions of sections 15 and 52 of PAIA providing for the voluntary disclosure of categories of records by a public body and private body, respectively;
- the notices issued in terms of sections 22 and 54 of PAIA regarding fees to be paid in relation to requests for access; and
- the regulations made in terms of section 92 of PAIA.

Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

A copy of the Guide is available for inspection upon request to the IO of the Vantage Entities during normal working hours. It is also available on the Regulator's website (accessible [here](#)) or by requesting it from the Regulator using the prescribed form (accessible [here](#)) or upon request to the IO using the prescribed form (accessible [here](#)).

Alternatively, the Information Officer has a copy of the Guide available in at least two of the official languages in South Africa at the Vantage Entities address available for inspection, at no fee, during normal working hours. Members of the public can also inspect or make copies of the Guide from the offices of the Regulator, at no fee, during normal working hours.

The Regulator is responsible for updating and making available the existing Guide that will facilitate ease of use of PAIA for requestors. Please direct any queries to the Regulator using the details below:

The Information Regulator	
Physical Address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191.
General Inquiries Email Address:	enquiries@inforegulator.org.za
Website:	https://inforegulator.org.za
Telephone:	010 023 5200
Toll Free	0800 017 160

6 CATEGORIES OF RECORDS WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

In accordance with section 52(1) of PAIA, the Vantage Entities have elected not to voluntarily make available to the public any categories of records that do not require the making of a request for access in terms of PAIA.

7 DESCRIPTION OF THE RECORDS AND RECORD CATEGORIES WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

Applicable Legislation
Basic Conditions of Employment Act, 75 of 1997
Broad-Based Economic Empowerment Act, 53 of 2003
Companies Act, 71 of 2008
Compensation for Occupational Injuries and Diseases Act, 130 of 1993
Employment Equity Act, 55 of 1998
Income Tax Act, 58 of 1962
Insurance Act, 63 of 2001
Labour Relations Act, 66 of 1995
Medical Schemes Act, 131 of 1998
Occupational Health and Safety Act, 85 of 1993

Applicable Legislation
Pension Funds Act, 24 of 1956
Promotion of Access to Information Act, 2 of 2000
Protection of Personal Information Act, 4 of 2013
Skills Development Levies Act, 9 of 1999
South African Revenue Services Act, 34 of 1997
Unemployment Insurance Contributions Act, 4 of 2002
Value Added Tax Act No. 89 of 1991

Subject of Information	Category of Information
See records listed under Labour Relations Act, 66 of 1995.	People & Culture
BBBEE Verification Certificate.	Corporate Governance
Incorporation and reorganisation records (including Memorandum of Incorporation). • Company registers, share certificates and other statutory registers. • Notices and minutes of board meetings and resolutions. • Records relating to the appointment of director(s), auditor(s), company secretary and other officer(s). • Documents on business processes. • Reports, including reports presented at annual general meetings. • Annual financial statements and any accounting records. • General policies and procedures. • Internal auditing/regulatory compliance records. • Compliance certifications. Applicable statutory documents.	Corporate Governance
• Employee health and safety, and accidents and injury records. • Registrations with the Department of Labour, Unemployment Insurance Fund, Compensation Fund and in terms of the Skills Development Levies Act.	Operational / Facilities
Employment Equity Plan	People & Culture
• Income tax returns • Pay As You Earn (PAYE) records. • Records of payments to SARS on behalf of employees. • IRP5 Forms • Documents issued to employees for income tax. • Statutory records	Finance / Tax
• Insurance claim records. • Insurance policies. • Details of insurance coverage, limits and insurers.	Legal / Compliance
• Recruitment and employee internal reference records and contact details. • Employment verification, immigration and expatriation records. • Employee personnel files and records. • Disciplinary procedures and records. • Grievance Procedures. • Employee development and training programs.	People & Culture

Subject of Information	Category of Information
- Employee forms and applications. - Leave records. - Background check (criminal records, credit checks). - Policies, standards, and procedures	
Employee medical aid records.	People & Culture
Employee health and safety, and accidents and injury records.	People & Culture
Employee benefits/compensation and benefit contribution arrangements, rules, and records.	People & Culture
- PAIA Manual - PAIA access to information requests. - Information Regulator's PAIA Guide. - PAIA compliance records	Legal / Compliance
- Information officer and deputy information officer registration certificates. - Data subject rights requests. - Data Protection and Privacy Policies. - Personal information compliance records.	Legal / Compliance
- Registrations with the Department of Labour, Unemployment Insurance Fund, Compensation Fund and in terms of the Skills Development Levies Act. - Employee skills development and training programs	People & Culture
See records listed under Income Tax Act, 58 of 1962.	Finance / Tax
- Registrations with the Department of Labour, Unemployment Insurance Fund, Compensation Fund and in terms of the Skills Development Levies Act. - UIF Returns.	Legal / Compliance
VAT Returns.	Finance / Tax

Note, whilst all reasonable endeavours have been made to provide a complete list of applicable legislation above, it is possible that the above list may be incomplete. Wherever it comes to the attention of the Vantage Entities that existing or new legislation allows a requestor access on a basis other than that set out in PAIA, POPIA, or the abovementioned legislation, the above list will be updated.

The records listed above are not automatically available and may be accessed only in accordance with PAIA, subject to any applicable grounds of refusal.

8 PROCESSING OF PERSONAL INFORMATION

8.1 Purpose of Processing Personal Information

- Customers / business partners / site visitors — contact details, relationship and transaction information, government ID data, online and technical data (IP address, device and access logs), CCTV and audio-visual recordings, biometric access data;

- Sales / marketing / customer engagement — contact details, communication preferences, transaction history, cookies and online identifiers used for marketing communications and personalised content;
- Site access / facilities / security — access logs, badge records, CCTV footage, call recordings, device and network logs, biometric identifiers used for physical and system access control;
- Human resources (workers) — contact details, personal characteristics, employee identifiers, employment records (contracts, performance, payroll, benefits, attendance, disciplinary), financial information, health and medical data, training and development records, inferred HR analytics (e.g. performance or retention indicators), emergency contact and dependants' data;
- Operations / facilities — maintenance records, operating procedures, site access logs, incident records;
- Workplace technology / monitoring — system and access logs, device data, user activity logs, location data (country-level), monitoring outputs including security alerts and usage data;
- Finance / tax — annual financial statements, accounting records, invoices, tax filings;
- Vendor / contractor management — supplier onboarding, due diligence, contracts, invoices;
- Real estate / development — land records, leases, easements, construction / project records;
- Recruitment — applicant contact details, CVs and candidate profiles (including LinkedIn), references and verification records, education and qualifications, background screening data, government ID data, interview and assessment records, limited health data (where relevant), audio-visual interview records;
- Compensation / finance (HR-related) — payroll data, bank account details, benefits and insurance records, expenses and transaction data;
- Health / wellbeing — occupational health data, fitness-for-work assessments, disability accommodations, absence and leave records, insurance and wellness program data;
- Compliance / investigations / regulatory — background checks, employment eligibility verification, audit and compliance records, incident and investigation files (including hotline reports), security and breach records, legal and regulatory reporting documentation;
- Everyday business operations — identity verification data, system administration records, cybersecurity monitoring data, fraud detection data, business continuity and backup records, audit and reporting datasets, contract enforcement records,

anonymised or aggregated datasets, and records supporting legal claims, governance, mergers and acquisitions.

8.2 Description of the Categories of Data Subjects and of the Information or Categories of Information Relating Thereto

Categories of Data Subjects	Personal Information that may be Processed
Vantage handles Personal Information about our customers, suppliers, business partners and other business professionals who visit our data centers or use our websites, applications, and customer portals.	• Contact Information: Such as name, address, email address, and telephone and/or mobile number. • Information Relating to Their Relationship with Vantage: Such as communication preferences and transaction information. • Government-issued identification information: Such as national ID number, driver's license number, passport number, other government-issued identifiers. • Online & Technical Information: Such as IP address, geo-location data, cookies, device information from devices that connect to our networks, system logs, including access logs and records of access attempts, records from access control devices, such as badge readers, records from technology monitoring programs, including suspicious activity alerts. • CCTV and Other Audio-Visual Information, as permitted by law: Such as photograph, video images, video conference records, CCTV recordings, call center recordings, voicemails. • Biometric identifiers as permitted by law: Such as fingerprints, mathematical representations of biometric identifier maintained for comparison. • Everyday Business Purposes: Such as identity verification data, system administration records, cybersecurity monitoring data, fraud detection data, business continuity and backup records, audit and reporting datasets, contract enforcement records, anonymised or aggregated datasets, and records supporting legal claims, governance, mergers and acquisitions.
Vantage handles Personal Information about our employees, officers, consultants, contractors, casual workers, and agency workers engaged to provide services to Vantage (collectively, our "Workers").	• Contact Information: Such as name, honorifics and titles, preferred form of address, mailing address, email address, telephone and/or mobile number, emergency contact details. • Personal Characteristics: Such as date of birth, gender, nationality. • Biometric identifiers as permitted by law: Such as fingerprints, mathematical representation of biometric identifier maintained for comparison. • Unique Identifiers: Such as company ID number, benefits program identifiers, system identifiers (usernames, online credentials). • Government-issued identification information: Such as national ID number, driver's license number, passport number, other government-

Categories of Data Subjects	Personal Information that may be Processed
	issued identifiers as may be needed for risk management or compliance (e.g., if you are a licensed professional, we will collect license number). Human Resource Information: Such as biographical data, resume or CV, including data from LinkedIn or similar profiles, references from former employers, education and degree information, marriage certificate, marital status, birth certificate, professional licenses, certifications and memberships and affiliations, personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status), interests and hobbies, information provided for company social and professional networks, including alumni programs, professional goals and interests. Transaction and Interaction Information: Such as dates of employment, re-employment eligibility, position, title, reporting information, work history information, time and attendance records, leave and absence records, salary/payroll records, benefit plan records, travel and expense records, training plan records, performance records, reviews and disciplinary records. Financial information: Such as bank account number and details, company-issued payment card information, including transaction records. Health Information: Such as medical information for job placement, including drug testing and fitness to work examinations, accommodation of disabilities, medical information for leave and absence management, emergency preparedness programs, wellness program data, information pertaining to utilization of health and disability insurance programs. Online & Technical Information: Such as device information from devices that connect to our networks, system logs, including access logs and records of access attempts, location of devices at a country level, records from access control devices, such as badge readers, records from technology monitoring programs, including suspicious activity alerts. Inferred and Derived Information: Such as advancement potential and success scores, flight risk and similar scores, benefits program utilization scores. Audio Visual Information, as permitted by law: Such as photograph, video images, video conference records, CCTV recordings, call center recordings, voicemails. Online Identifiers: Such as user IDs, cookies, user activity logs, IP address and social media profile. Children's data: We collect children's data pertaining to children under 16 from the parents or guardians of the children. We do not collect any personal information directly from children under age 16. Such information includes child's name, date of birth and relationship with the Worker. Compliance data: Such as employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, occupational safety records and worker's compensation program records, records relating to internal investigations, including compliance hotline reports, security clearance information, records of privacy and security incidents involving HR records, including any breach notifications. Everyday Business Purposes: Such as identity verification data, system administration records, cybersecurity monitoring data, fraud detection data,

Categories of Data Subjects	Personal Information that may be Processed
	business continuity and backup records, audit and reporting datasets, contract enforcement records, anonymised or aggregated datasets, and records supporting legal claims, governance, mergers and acquisitions.
Vantage handles Personal Information of Job Applicants as part of our recruitment process.	• Contact Information: Such as name, honorifics and titles, preferred form of address, mailing address, email address, telephone and/or mobile number, emergency contact details. • Personal Characteristics: Such as date of birth, gender, nationality. • Government-issued identification information: Such as national ID number, driver's license number, passport number, other government-issued identifiers as may be needed for risk management or compliance (e.g., if you are a licensed professional, we will collect license number). • Human Resource Information: Such as biographical data, resume or CV, including data from LinkedIn or similar profiles, references from former employers, education and degree information, marriage certificate, marital status, birth certificate, professional licenses, certifications and memberships and affiliations, personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status), interests and hobbies, information provided for company social and professional networks, including alumni programs, professional goals and interests. • Financial information: Such as bank account number and details, company-issued payment card information, including transaction records. • Health Information: Such as medical information for job placement, including drug testing and fitness to work examinations, accommodation of disabilities, medical information for leave and absence management, emergency preparedness programs, wellness program data, information pertaining to utilization of health and disability insurance programs. • Audio Visual Information, as permitted by law: Such as photograph, video images, videoconference records, CCTV recordings, call center recordings, voicemails. • Online Identifiers: Such as user IDs, cookies, user activity logs, IP address and social media profile. • Compliance data: Such as employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, occupational safety records and worker's compensation program records, records relating to internal investigations, including compliance hotline reports, security clearance information, records of privacy and security incidents involving HR records, including any breach notifications. • Everyday Business Purposes: Such as identity verification data, system administration records, cybersecurity monitoring data, fraud detection data, business continuity and backup records, audit and reporting datasets, contract enforcement records, anonymised or aggregated datasets, and records supporting legal claims, governance, mergers and acquisitions.

The recipients or categories of recipients to whom the personal information may be supplied

The Vantage Entities may share the personal information listed above with the following third parties:

- **Internal Disclosures:** The Personal Information may be shared with other Vantage entities.
- **Third Party Disclosures:** The Personal Information may be shared with third-party service providers and/or suppliers (e.g. IT, digital and technology providers).
- **Consultants and Advisors:** The Personal Information may be shared with legal counsel, compliance consultants and business auditors, or business partners.
- **Commercial Disclosures:** The Personal Information may be shared with suppliers.
- **Disclosures Required by Law:** The Personal Information may be shared with law enforcement agencies and regulators.

Planned transborder flows of personal information

The Vantage Entities may transfer Personal Information under its control to organisations, service providers, and other Vantage Data Centers entities outside of South Africa for the purposes of hosting, support, HR administration, IT security, legal, compliance and business operations. Such transfers may include employee, recruitment, customer contact, visitor access and website / IT usage data. The Vantage entities will take steps to ensure that Operators (as defined in POPIA) in foreign countries are bound by laws, binding corporate rules or binding agreements that provide an adequate level of protection of Personal Information and uphold the principles for reasonable and lawful processing of Personal Information, in terms of section 72 of POPIA.

General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information

The Vantage Entities maintain appropriate technical and organisational security measures, including access controls, role-based access, least-privilege permissions, multi-factor authentication where appropriate, encryption, logging and monitoring, vulnerability and patch management, anti-malware controls, backups and recovery measures, physical security controls, vendor management controls, employee confidentiality obligations, and incident response processes.

The Vantage Entities are committed to ensuring that these information security measures which protect the Personal Information are continuously reviewed and updated where necessary.

9 AVAILABILITY OF THE MANUAL

A copy of the Manual is available for inspection upon request to the IO of the Vantage Entities during normal working hours using the details provided earlier in this Manual. It is also available:

- on the Regulator's website;
- at vantage-dc.com/PAIA-Manual
- for public inspection during normal business hours at Merlot House, The Vineyards Office Estate, 99 Jip De Jager Drive, Bellville, Western Cape, South Africa, 7530.
- from the Regulator, upon request.

The Vantage Entities reserve the right to withhold access to the record until the prescribed fee, in terms of section 54 of PAIA read with regulation 8 and Annexure B of the PAIA Regulations, is paid.

10 PROCEDURE FOR REQUESTING ACCESS TO INFORMATION IN TERMS OF PAIA

Requests for access to records must be made using the prescribed [Form 2](#) in terms of Regulation 7 of the PAIA Regulations and must be submitted to the IO or DIO using the contact details in this Manual. [Forms 3 \(Outcome of Request and of Fees Payable\)](#) and [5 \(Complaint Form\)](#) are also linked for reference. A requester must identify the right sought to be exercised or protected, explain why the requested record is required for that purpose and provide sufficient detail on the prescribed form to allow the Vantage Entities to identify the record or records which have been requested and the identity of the requester.

A request must comply with all the procedural requirements as contained in section 53 of PAIA relating to a Request for Access to a Record.

The Vantage Entities will process the Request for Access and notify the requestor of the decision within 30 days of receipt of the Request for Access, unless the Request for Access is of such a nature that an extension of the prescribed time limit is necessitated in accordance with section 57 of PAIA. In the case of an extension of the time limit, the requestor has the right to lodge a complaint with the Regulator in accordance with PAIA and POPIA by completing the prescribed forms.

There are various grounds upon which the Vantage Entities may or must refuse a Request for Access to a Record in accordance with Chapter 4 of PAIA, which include:

- that access would result in the unreasonable disclosure of Personal Information about a third party;
- to protect the commercial information of a third party or of the Vantage Entities;

- that it is necessary to protect the confidential information of a third party;
- to protect the safety of individuals or property;
- that a record constitutes privileged information for the purpose of legal proceedings; and
- to protect the research information of a third party or the Vantage Entities.

Requests for information that are clearly frivolous or vexatious, or which involve unreasonable diversion of resources shall be refused.

All requests for information will be assessed on their own merits and in accordance with applicable laws.

Once the IO has heard all the submissions, the IO will decide as to whether or not access to the Record will be granted. If access is granted the requestor must then be granted access to the Record within 30 days of being informed of the decision.

If the request for access is successful, an access fee may be required for the search, reproduction and/or preparation of the Record(s). The access fee must be paid prior to access being given to the requested Record(s).

The Vantage Entities are required to inform a requester in writing of its decision in relation to a request (section 56 of PAIA). If the requester wishes to be informed of a decision in another manner as well, this must be set out in the request and the relevant details must be included, to allow the Vantage Entities to inform the Requester in the preferred manner.

If the IO does not grant the requestor access to the Record the requestor is entitled in accordance with sections 56(3) (c) and 78 of PAIA to apply to a court for relief within 180 days of notification of the decision for appropriate relief, such as an order compelling the Record or Records requested to be made available to the requestor or for another appropriate order. The court will determine whether the records should be made available or not.

The requestor may also approach the Regulator and lodge a complaint in accordance with section 74 of POPIA in the prescribed form and email to: POPIAComplaints@inforegulator.org.za and in accordance with section 77(a) of PAIA and email to: PAIAComplaints@inforegulator.org.za.

If a requested record cannot be found or if the records do not exist, the IO shall, by way of an affidavit or an affirmation, notify the requestor that it is not possible to give access to the requested record.

11 DOCUMENT CONTROL

Revision History

Date	Version	Revised Sections	Edited by	Reason
02/11/2026	0.1	All	Deputy Information Officer	Initial Publication

Annual Review

Last Annual Review:	02/11/2026	Next Annual Review	03/01/2028
----------------------------	------------	---------------------------	------------

This Manual will be updated on a regular basis in accordance with the requirements of section 51(2) of PAIA.