PAIA Manual

Document Control

Document title:	PAIA Manual
Document identifier:	AST-LG-PAIA-01
Version number:	5
Review date:	27/05/2026
Next review:	27/05/2027

ASCENT TECHNOLOGY (PTY) LTD

Registration number: 2002/001242/07

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

Contents

1. Introduction

Ascent Technology (Pty) Ltd (hereinafter referred to as 'Ascent' or the 'the organisation') conducts business as an Enterprise Database Management Services organisation delivering end-to-end, cost-effective, high-quality database management, database administration co/outsourcing, database consulting, resource contracting, database license consulting / sales, services, and support. This Promotion of Access to Information Manual (hereafter 'the Manual') provides an outline of the type of records and personal information it holds and explains how to submit requests for access to these records in terms of the Promotion of Access to Information Act 2 of 2000 (hereinafter referred to as 'PAIA'). In addition, it explains how to access, or object to, personal information held by the organisation, or request correction of the personal information, in terms of paragraphs 23 and 24 of the Protection of Personal Information Act 4 of 2013 (hereafter 'POPIA'). The PAIA and POPIA give effect to everyone's constitutional right to access to information held by the private sector or public bodies if the record or personal information is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest. Requests shall be made following the prescribed procedures, at the rates provided. The forms and tariffs are dealt with in section 6. This PAIA Manual is published in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended).

2. Terms and definitions

Term / Abbreviation / Acronym	Definitions
Access fee	The prescribed fee payable by a requester for the search, preparation, reproduction, and provision of access to a record, where applicable.
The organisation	Ascent, being the private body to which this Manual applies.
Confidentiality	The principle that information is protected against unauthorised access, disclosure, or use.
Integrity	The principle that information is accurate, complete, and protected against unauthorised or improper alteration.
Availability	The principle that information and systems are accessible and usable by authorised persons when required.
Consent	Any voluntary, specific, and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to them.
Data subject	The person to whom personal information relates, including, where applicable, clients, customers, employees, applicants, suppliers, contractors, service providers, visitors, website users, and other relevant persons.
Information Officer / IO	The head of the private body, or the person duly authorised or designated as the Information Officer,

	responsible for ensuring compliance with PAIA and POPIA.
DIO / Deputy Information Officer	The person appointed or designated to assist the Information Officer with the performance of duties and responsibilities under PAIA and POPIA, including access to information requests and personal information protection matters.
Information Regulator / IR / Regulator	The Information Regulator established in terms of POPIA and empowered to monitor and enforce compliance with PAIA and POPIA.
Intellectual property	Intellectual property owned, licensed, developed, used, or held by Ascent, including copyright, trademarks, trade secrets, methodologies, templates, software, source files, scripts, storyboards, course material, learning content, multimedia content, designs, graphics, videos, training materials, and other proprietary materials.
Manual	This PAIA Manual prepared in accordance with section 51 of PAIA.
Operator	A person or entity that processes personal information for Ascent in terms of a contract or mandate, without coming under the direct authority of Ascent.
PAIA	Promotion of Access to Information Act 2 of 2000, as amended.
Personal information	Information relating to an identifiable, living natural person, and where applicable, an identifiable existing juristic person, including contact details, identification details, employment information, financial information, health information, online identifiers, correspondence, opinions, and other information as defined in POPIA.
Special personal information	Special categories of personal information as contemplated under POPIA, including information relating to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour, where applicable.
Personal requester	A requester who requests access to a record containing personal information about themselves.
Requester	Any person, including a natural person, juristic person, public body, or person acting on behalf of another person, who requests access to a record of Ascent in terms of PAIA.
POPIA	Protection of Personal Information Act 4 of 2013, as amended.
Prescribed fee	Any fee prescribed in terms of PAIA and its regulations, including request fees, access fees, reproduction fees, search and preparation fees, and any applicable deposit.

Private Body	A natural person, partnership, juristic person, or other body contemplated in PAIA, which carries on any trade, business, or profession, and to which PAIA applies.
Processing	Any operation or activity concerning personal information, including collection, receipt, recording, organisation, storage, updating, modification, retrieval, use, dissemination, transfer, restriction, deletion, destruction, or any other handling of personal information.
Record	Any recorded information, regardless of form or medium, which is in the possession or under the control of Ascent, whether or not it was created by Ascent.
Request fee	The prescribed fee that may be payable by a requester before a request for access to a record is processed, where applicable.
Third party	Any person or entity other than the requester and Ascent, including a natural person, juristic person, supplier, client, employee, regulator, public body, or other external party.
Transborder flow	The transfer, storage, hosting, access, or processing of personal information outside the Republic of South Africa.

3. Purpose of the PAIA Manual

This PAIA Manual is useful for the public to:

3.1 Check the categories of records held by a body that are available without a person having to submit a formal PAIA request.

3.2 Have sufficient understanding of how to request access to a record of the body, by describing the subjects on which the body holds records and the categories of records held on each subject.

3.3 Know the description of the records of the body which are available under any other legislation.

3.4 Access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access.

3.5 Know the description of the guide on how to use PAIA, as updated by the Regulator, and how to obtain access to it.

3.6 Know if the body will process personal information, the purpose of the processing of personal information, and the description of the categories of data subjects and the information or categories of information relating thereto.

3.7 Know the description of the categories of data subjects and the information or categories of information relating thereto.

3.8 Know the recipients or categories of recipients to whom the personal information may be supplied.

3.9 Know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied.

3.10 Know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

4. Key contact details for access to information of Ascent

Company contact details in terms of section 51 of PAIA:

Information Officer:

Imraan Sallie

138 West St, Sandown, Johannesburg, 2031

imraan.sallie@ascent.tech

+27 11 745 1340

Deputy Information Officer:

Joelene van der Merwe

138 West St, Sandown, Johannesburg, 2031

joelene.vandermerwe@ascent.tech

+27 11 745 1340

Information Regulator:

010 023 5200

enquiries@inforegulator.org.za

Woodmead North Office Park

54 Maxwell Drive

Woodmead

Johannesburg

2191

5. Guide on how to use PAIA

5.1 The Information Regulator, in terms of section 10(1) of PAIA (as amended), has updated and published the revised Guide on how to use PAIA. The Guide is available in a clear, accessible format to assist anyone who wishes to exercise their rights under PAIA and POPIA.

5.2 The Guide is available in each of the official languages and braille.

5.3 The aforesaid Guide contains the description of:

5.3.1 The objects of PAIA and POPIA.

5.3.2 The postal and street address, telephone, and fax number and, if available, electronic mail address of:

5.3.2.1 The Information Officer of every public body, and

5.3.2.2 Every Deputy Information Officer of every public and private body is designated in terms of section 17(1) of PAIA[1] and section 56 of POPIA[2].

5.3.3 The manner and form of a request for:

5.3.3.1 Access to a record of a public body contemplated in section 11[3]; and

5.3.3.2 Access to a record of a private body contemplated in section 50[4];

5.3.4 The assistance available from the IO of a public body in terms of PAIA and POPIA.

5.3.5 The assistance available from the Regulator in terms of PAIA and POPIA.

5.3.6 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:

5.3.6.1 An internal appeal;

5.3.6.2 A complaint to the Regulator; and

5.3.6.3 An application with a court against a decision by the information officer 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.

5.3.7 The provisions of sections 14[5] and 51[6] require a public body and a private body, respectively, to compile a manual, and to obtain access to it.

---

1 Section 17(1) of PAIA – For the purposes of PAIA, each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as deputy information officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.

2 Section 56(a) of POPIA – Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.

3 Section 11(1) of PAIA – A requester must be given access to a record of a public body if that requester complies with all the procedural requirements in PAIA relating to a request for access to that record; and access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

4 Section 50(1) of PAIA A requester must be given access to any record of a private body if: a) that record is required for the exercise or protection of any rights; b) that person complies with the procedural requirements in PAIA relating to a request for access to that record; and c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

5 Section 14(1) of PAIA – The information officer of a public body must, in at least three official languages, make available a manual containing information listed in paragraph 4 above.

6 Section 51(1) of PAIA – The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.

5.3.8 The provisions of sections 15[7] and 52[8] provide for the voluntary disclosure of categories of records by a public body and a private body, respectively.

5.3.9 The notices issued in terms of sections 22[9] and 54[10] regarding fees to be paid concerning requests for access; and

5.3.10 The regulations made in terms of section 92[11].

5.4 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.

5.5 The Guide is available from the Information Regulator's website. For ease of access, the organisation has made the English version of the Guide available on its website. A copy of the Guide is also available for public inspection during normal business hours at the organisation's head office in the following two official languages: English and Afrikaans.

---

7 Section 15(1) of PAIA – The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access.

8 Section 52(1) of PAIA – The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access.

9 Section 22(1) of PAIA – The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

10 Section 54(1) of PAIA – The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

11 Section 92(1) of PAIA provides that – The Minister may, by notice in the Gazette, make regulations regarding –

(a) any matter which is required or permitted by this Act to be prescribed.
(b) any matter relating to the fees contemplated in sections 22 and 54.
(c) any notice required by this Act.
(d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and
(e) any administrative or procedural matter necessary to give effect to the provisions of this Act."

6. Categories of records that are available without requiring a formal information access request

The records listed below are generally available without a formal PAIA request and may be accessed through the organisation's website or provided upon informal request. Access remains subject to availability and any applicable confidentiality, privacy, copyright, or legal restrictions.

Category of records	Types of record	Available on the website	Available upon request
Company information	Company profile, business overview, contact details, physical address, and general company information.	X	X
Products and services information	Service offerings, product information, brochures, catalogues, course or programme outlines, and pricing information where publicly available.	X	X
Website and digital information	Website content, privacy notice, cookie notice, terms of use, website disclaimers, and online forms.	X	X
PAIA and POPIA information	PAIA Manual, Information Officer contact details, privacy notices, data subject request forms, and PAIA request forms.	X	X
Marketing and communication information	Newsletters, promotional material, public announcements, event notices, webinar invitations, and social media content.	X	X
Human resources information	Publicly advertised vacancies, recruitment notices, and general career information.	X	X
Contact and enquiry information	General enquiry forms, complaint forms, contact forms, and customer support or service contact details.	X	X

7. Description of the records of Ascent which are available in accordance with any other legislation

The records listed below are created, maintained, submitted, and/or made available in accordance with applicable South African legislation. Inclusion of a record in this section does not mean that the record is automatically or publicly available. Access to any record remains subject to PAIA, POPIA, confidentiality obligations, and any other applicable legal grounds for refusal or restriction.

Category of records	Applicable legislation	Access requirement
Memorandum of Incorporation	Companies Act 71 of 2008	May require a formal request
Company registration documents	Companies Act 71 of 2008	May require a formal request
Company registers and statutory company records	Companies Act 71 of 2008	May require a formal request
Shareholder records, where applicable	Companies Act 71 of 2008	May require a formal request
Director records and resolutions	Companies Act 71 of 2008	Formal request required
PAIA Manual	Promotion of Access to Information Act 2 of 2000	Publicly available
PAIA request records	Promotion of Access to Information Act 2 of 2000	Formal request required
POPIA compliance records	Protection of Personal Information Act 4 of 2013	Formal request required
Privacy notices	Protection of Personal Information Act 4 of 2013	Publicly available
Data subject request records	Protection of Personal Information Act 4 of 2013	Formal request required
Employment contracts and employee records	Basic Conditions of Employment Act 75 of 1997	Formal request required
Employment equity records, where applicable	Employment Equity Act 55 of 1998	Formal request required
Skills development and training records, where applicable	Skills Development Act 97 of 1998; Skills Development Levies Act 9 of 1999	Formal request required
Occupational health and safety records	Occupational Health and Safety Act 85 of 1993	Formal request required

Compensation for occupational injuries and diseases records	Compensation for Occupational Injuries and Diseases Act 130 of 1993	Formal request required
Tax records and returns	Income Tax Act 58 of 1962; Tax Administration Act 28 of 2011	Formal request required
VAT records	Value-Added Tax Act 89 of 1991	Formal request required
PAYE, UIF and SDL records, where applicable	Income Tax Act 58 of 1962; Unemployment Insurance Contributions Act 4 of 2002; Skills Development Levies Act 9 of 1999	Formal request required
Accounting records and financial statements	Companies Act 71 of 2008; Tax Administration Act 28 of 2011	Formal request required
B-BBEE records	Broad-Based Black Economic Empowerment Act 53 of 2003	May require formal request
Consumer-related records, where the body supplies goods or services to consumers as defined in the Act	Consumer Protection Act 68 of 2008	Formal request required
Customer records and contracts	Companies Act 71 of 2008; Protection of Personal Information Act 4 of 2013	Formal request required
Supplier records and contracts	Companies Act 71 of 2008; Protection of Personal Information Act 4 of 2013	Formal request required
Electronic communications and transaction records	Electronic Communications and Transactions Act 25 of 2002	Formal request required

8. Description of the subjects on which the body holds records and categories of records held on each subject by Ascent

The table below describes the subjects on which the body holds records and the categories of records held under each subject. Access to any of these records is subject to PAIA, POPIA, confidentiality obligations, and any other applicable legal grounds for refusal or restriction.

Subjects on which the body holds records	Categories of records
Strategic and Governance Records	Strategic plans, business plans, operational plans, policies, procedures, management reports, meeting minutes, resolutions, organisational structure records.
Company Secretarial and Statutory Records	Company registration documents, Memorandum of Incorporation, statutory registers, shareholder records, director records, CIPC records, and company resolutions.
Human Resources Records	HR policies and procedures, employment contracts, employee records, leave records, disciplinary records, performance records, training records, recruitment records, and advertised posts.
Finance and Accounting Records	Accounting records, invoices, statements, receipts, payment records, payroll records, tax records, VAT records, budgets, financial reports, and audited financial statements, where applicable.
Sales and Marketing Records	Marketing materials, client proposals, quotations, service brochures, newsletters, website content, social media content, and client communication records.
Client and Customer Records	Client agreements, customer records, project records, service delivery records, complaints, enquiries, customer correspondence, customer feedback.
Supplier and Procurement Records	Supplier records, supplier agreements, purchase orders, procurement records, service level agreements, supplier invoices, supplier correspondence.
Legal and Compliance Records	Contracts, legal opinions, compliance registers, regulatory correspondence, PAIA records, POPIA records, risk registers, audit records, and internal compliance assessments.
Information Technology Records	IT policies, system access records, user account records, asset registers, software licences, cybersecurity records, backup records, system logs, and incident reports.
Data Protection and Privacy Records	Privacy notices, consent records where applicable, data subject request records, personal information impact assessments, operator agreements, data breach records, and information asset registers.

Occupational Health and Safety Records	Health and safety policies, risk assessments, incident reports, inspection records, emergency plans, first aid records, and training records.
Information Security and Cybersecurity Records	Information security policies, risk assessments, risk treatment records, Statement of Applicability, access control records, incident records, asset registers, backup and business continuity records, internal audit records, management review records, corrective action records, and ISO/IEC 27001 certification-related records.
Project and Service Delivery Records	Project plans, implementation records, deliverables, project schedules, progress reports, client sign-offs, meeting records, and close-out reports.
Training Records	Training materials, attendance registers, and assessment records
Communications and Correspondence	Emails, letters, notices, internal announcements, external correspondence, stakeholder communication records.
Insurance and Risk Records	Insurance policies, claims records, risk assessments, risk registers, business continuity records, and incident records.
Facilities and Asset Records	Asset registers, maintenance records, lease agreements, office records, access control records, and equipment records.

9. Processing of personal information

Ascent is committed to the lawful, fair, transparent, and responsible processing of personal information in accordance with POPIA and other applicable laws.

Ascent processes personal information only where there is a lawful basis to do so and where such processing is necessary for legitimate business, operational, legal, contractual, employment, compliance, and service delivery purposes. Personal information may be collected, used, stored, shared, transferred, archived, updated, corrected, deleted, or destroyed in accordance with applicable legal requirements and Ascent's internal policies and procedures.

9.1 Purpose of processing personal information

Ascent processes personal information only where necessary and permitted by law. The purposes for which personal information may be processed include, but are not limited to, the following:

9.1.1 to provide, manage, administer, and improve products, services, solutions, consulting, support, and related offerings requested by clients, customers, users, or other data subjects;

9.1.2 to verify, identify, and communicate with data subjects when they contact, engage with, or request information from Ascent;

9.1.3 to create, maintain, update, and manage records relating to clients, customers, employees, applicants, suppliers, contractors, service providers, business partners, and other relevant stakeholders;

9.1.4 to prepare, issue, manage, and administer quotations, proposals, agreements, contracts, project documentation, service delivery records, client engagements, and related business relationships;

9.1.5 to process job applications, curriculum vitae, interview records, assessment information, employment offers, reference checks, and other recruitment-related information;

9.1.6 to manage employment, apprenticeship, internship, contractor, and workplace-related matters, including payroll, benefits, leave administration, performance management, training, disciplinary processes, employee development, and general workforce administration;

9.1.7 to arrange and manage meetings, travel, accommodation, events, training sessions, workshops, webinars, and related logistical arrangements;

9.1.8 to perform administrative, operational, financial, accounting, billing, payment, debt collection, auditing, tax, and statutory reporting functions;

9.1.9 to comply with applicable legal, regulatory, contractual, governance, audit, risk management, recordkeeping, and compliance obligations;

9.1.10 to manage occupational health and safety, workplace incidents, emergency response, business continuity, physical security, and access to Ascent's premises, facilities, systems, platforms, and assets;

9.1.11 to transact, communicate, and manage relationships with suppliers, service providers, contractors, business partners, professional advisers, regulators, and other authorised third parties;

9.1.12 to monitor, secure, support, maintain, and improve Ascent's information systems, websites, applications, platforms, networks, infrastructure, facilities, and business operations;

9.1.13 to detect, prevent, investigate, respond to, and report fraud, corruption, misconduct, security incidents, unlawful activity, money laundering, cyber incidents, data breaches, or other actual or suspected risks;

9.1.14 to manage complaints, enquiries, requests, disputes, claims, litigation, investigations, regulatory engagements, and legal processes;

9.1.15 to conduct internal reporting, analytics, research, service improvement, customer relationship management, business development, and operational planning activities;

9.1.16 to develop, manage, deliver, and improve learning content, multimedia content, induction material, training programmes, assessments, certificates, digital platforms, and related intellectual property or service deliverables;

9.1.17 to market Ascent's products, services, events, content, publications, and solutions, where permitted by law or where the required consent has been obtained; and

9.1.18 for any other lawful purpose directly related to Ascent's business activities, provided that such processing is permitted in terms of applicable law.

9.2 Description of the categories of data subjects and personal information processed

The categories of data subjects in respect of whom Ascent may process personal information, and the nature or categories of personal information that may be processed, are set out below.

Categories of data subjects	Personal Information that may be processed
Clients, customers, and potential clients	Names, surnames, identity or registration numbers where required, contact details, email addresses, telephone numbers, physical and postal addresses, company details, job titles, departments, service requests, proposals, quotations, agreements, correspondence, billing information, payment information, opinions, feedback, complaints, and records relating to services requested or provided.
Employees	Names, surnames, identity or passport numbers, contact details, addresses, demographic information where required by law, next-of-kin details, employment contracts, job titles, qualifications, employment history, payroll information, tax information, banking details, leave records, performance records, disciplinary records, training records, benefits information, medical information where necessary, disability information where applicable, health and safety records, access control records, surveillance records, and workplace communication records.
Job applicants and potential employees	Names, surnames, identity or passport numbers, contact details, addresses, curriculum vitae, application forms, qualifications, employment history, references, interview records, assessment results, background screening results, criminal checks where permitted by law, credit checks where relevant and permitted, and correspondence relating to recruitment.
Suppliers, service providers, vendors and contractors	Names, surnames, identity or registration numbers, VAT numbers, contact details, business addresses, company information, banking details, tax information, B-BBEE information where applicable, agreements, purchase orders, invoices, payment records, supplier onboarding records, supplier performance records, correspondence, and details of supplier representatives.

Directors and company representatives	Names, surnames, identity or passport numbers, contact details, addresses, appointment records, statutory records, declarations of interest, resolutions, meeting records, CIPC-related records, and correspondence.
Business partners and professional advisers	Names, surnames, contact details, email addresses, telephone numbers, organisation details, job titles, contractual information, correspondence, meeting records, opinions, advice, reports, invoices, and payment information.
Visitors and guests	Names, surnames, contact details, organisation represented, person visited, date and time of visit, access records, visitor registers, and CCTV or surveillance footage.
Website users, online users, and social media users	Names, surnames, contact details where provided, email addresses, online identifiers, IP addresses, device information, cookies, usage data, enquiry details, form submissions, marketing preferences, communication records, and social media interaction records.
Event, training, and webinar participants	Names, surnames, contact details, email addresses, telephone numbers, organisation details, job titles, attendance records, registration information, dietary or accessibility requirements (where applicable), assessment records, certificates, photographs, video or audio recordings (where applicable), feedback, and correspondence.
Complainants, enquirers, and other correspondents	Names, surnames, contact details, email addresses, telephone numbers, enquiry details, complaint details, correspondence, supporting documents, call records where applicable, and records relating to the resolution of enquiries, complaints, or requests.
Regulators, auditors, and public authorities	Names, surnames, contact details, job titles, organisation details, correspondence, audit records, compliance records, statutory submissions, inspection records, investigation records, and regulatory communication records.
Emergency contacts, dependants, and beneficiaries	Names, surnames, contact details, relationship to the employee or relevant data subject, identity numbers where required, benefit information, medical aid information where applicable, and emergency contact information.

9.3 Recipients or categories of recipients to whom personal information may be supplied

Ascent may, where necessary and permitted by law, supply personal information to the following recipients or categories of recipients for lawful business, operational, contractual, regulatory, compliance, employment, security, and service delivery purposes.

Category of personal information	Recipients or categories of recipients to whom the personal information may be supplied
Identity information, contact details, employment information, tax information, payroll information, and statutory employment records	SARS, Department of Employment and Labour, UIF, Compensation Fund, payroll service providers, auditors, accountants, banks, medical aid providers, insurers, and authorised Ascent personnel.
Identity information, criminal history information, qualification records, references, employment history, and background screening information	South African Police Service, background screening providers, credit bureaus where permitted, South African Qualifications Authority, qualification verification bodies, and authorised Ascent personnel.
Client, customer, learner, student, delegate, training, assessment, attendance, certification, and course completion information	Clients, sponsoring organisations, employers, accreditation bodies, certification bodies, moderators, assessors, training providers, learning platform providers, and authorised Ascent personnel.
Supplier, vendor, contractor, invoice, tax, VAT, B-BBEE, banking, payment, and onboarding information	SARS, banks, payment service providers, auditors, accountants, legal advisers, procurement personnel, regulators, where applicable, and authorised Ascent personnel.
Financial, billing, accounting, audit, tax, and payment information	SARS, banks, payment service providers, auditors, accountants, tax advisers, legal advisers, courts, and authorised Ascent personnel.
Health and safety information, incident records, medical information where necessary, disability information where applicable, emergency contact details, and workplace injury records	Department of Employment and Labour, Compensation Fund, emergency responders, insurers, legal advisers, and authorised Ascent personnel.
Access control records, visitor records, CCTV footage, system access records, security logs, device information, and incident records	Security service providers, IT service providers, cybersecurity providers, cloud/hosting providers, forensic investigators, law enforcement authorities, where required, the Information Regulator, where applicable, insurers, and authorised Ascent personnel.
Website, platform, communication, enquiry, marketing preference, cookie,	Website hosting providers, IT service providers, cloud providers, analytics providers, CRM providers, communication platforms, marketing service providers,

analytics, and social media interaction information	social media platforms, and authorised Ascent personnel.
Complaints, disputes, claims, litigation, regulatory requests, investigation records, and supporting documents	Legal advisers, auditors, insurers, regulators, ombuds, courts, tribunals, law enforcement authorities, professional advisers, and authorised Ascent personnel.
Personal information processed by contracted operators or service providers on behalf of Ascent	IT providers, cloud providers, software providers, hosting providers, payroll providers, payment processors, document storage providers, marketing providers, and other authorised operators acting under a written agreement.

Ascent will only supply personal information to recipients where there is a lawful basis to do so, where the disclosure is necessary for the purposes for which the information was collected or subsequently processed, where required or authorised by law, or where the data subject has provided consent, where applicable. Recipients who process personal information on behalf of Ascent must do so in accordance with applicable data protection, confidentiality, and security requirements.

9.4 Planned transborder flows of personal information

Ascent will only transfer personal information across the borders of the Republic of South Africa where the relevant business transaction, operational requirement, contractual obligation, legal requirement, or specific circumstances require such transborder processing, or where the data subject has consented to the transfer, where required.

Where any transborder transfer of personal information becomes necessary, Ascent will ensure that such transfer is carried out in accordance with POPIA and other applicable legal requirements. Ascent will take reasonable steps to ensure that any operators, service providers, or third parties processing personal information outside South Africa are subject to appropriate safeguards, including applicable laws, binding corporate rules, contractual obligations, operator agreements, confidentiality obligations, or other measures that provide an adequate level of protection for the lawful and reasonable processing of personal information. Where notification or consent is required, Ascent will provide the data subject with appropriate information regarding the nature of the transfer, the categories of personal information concerned, the recipient or category of recipient, and the applicable safeguards, where reasonably practicable.

9.5 Information security measures implemented to ensure the confidentiality, integrity, and availability of information

Ascent implements reasonable and appropriate technical, organisational, administrative, and physical safeguards to protect personal information in its possession or under its control against unauthorised access, unlawful processing, loss, damage, destruction, alteration, disclosure, or misuse. The organisation maintains an Information Security Management System aligned to ISO/IEC 27001:2022 and applies information security controls designed to preserve the confidentiality, integrity, and availability of information. These controls are implemented having regard to the nature of the personal information processed, the risks associated with such

processing, applicable legal and contractual requirements, and generally accepted information security practices.

The security measures implemented or under implementation include, where applicable, information security policies and procedures, access control measures, user authentication controls, password controls, multi-factor authentication, antivirus and anti-malware protection, encryption, secure transmission methods, network and endpoint security controls, patch and vulnerability management, backup and recovery controls, business continuity and disaster recovery arrangements, physical security controls, secure retention and disposal practices, system monitoring and logging, incident management procedures, confidentiality undertakings, and employee awareness and training.

Access to personal information is restricted to authorised employees, contractors, operators, and service providers who require access for legitimate business, operational, contractual, legal, or service delivery purposes. Appropriate access management controls are applied to ensure that users are granted access only to information and systems necessary for the performance of their functions.

The organisation takes reasonable steps to ensure that operators and service providers who process personal information on its behalf are subject to appropriate contractual, confidentiality, data protection, and information security obligations. Where applicable, such parties are required to implement safeguards appropriate to the nature of the personal information processed and the risks associated with such processing.

Procedures are in place to identify, report, assess, investigate, contain, and respond to actual or suspected information security incidents or personal information breaches. Where required by law, the Information Regulator and affected data subjects will be notified of security compromises in accordance with POPIA.

Ascent reviews and improves its information security measures on an ongoing basis through risk assessments, internal controls, audits, monitoring, corrective actions, management reviews, awareness activities, and continual improvement processes aligned to its ISO/IEC 27001:2022 Information Security Management System.

10. Access to records and grounds for refusal

10.1 Grounds of refusal to access to records

Access to records held by Ascent is governed by PAIA, POPIA, this Manual, and any other applicable law. A requester may request access to a record held by or under the control of Ascent, provided that the requester complies with the procedural requirements set out in PAIA and provides sufficient information to enable the Information Officer to identify the record requested.

Where a requester seeks access to their own personal information, such request will be considered in accordance with PAIA, POPIA, proof of identity requirements, applicable fees, and any lawful grounds for refusal. Where a request is made on behalf of another person, the requester must provide proof of authority to act in that capacity, to the reasonable satisfaction of the Information Officer.

Where a requester seeks access to records other than their own personal information, the requester must clearly identify the right they seek to exercise or protect and must explain why the requested record is reasonably required for the exercise or protection of that right. The right of access applies only to records that exist and are held by or under the control of Ascent at the time the request is made. Ascent is not required to create a record that does not exist.

10.2 Request procedure

A requester must complete the prescribed **Form 2: Request for Access to Record (as attached in Annexure A)** and submit it to the Information Officer using the contact details provided in this Manual. The request must contain sufficient detail to enable the Information Officer to identify the requester, the requested record, the form in which access is required, and the right that the requester seeks to exercise or protect.

The requester may be required to provide proof of identity and, where applicable, proof of authority to act on behalf of another person, including a mandate, power of attorney, company resolution, or other acceptable proof. Where a request does not contain sufficient information, or where the requester has not properly identified the record or the right sought to be exercised or protected, Ascent may request further information before processing the request.

If a requester is unable to complete the prescribed form because of illiteracy, disability, or any other reasonable cause, the request may be made orally. In such circumstances, the Information Officer may assist the requester by reducing the request to writing.

10.3 Requests relating to third parties

Where a request relates to a record that contains information about a third party, Ascent may be required to notify that third party in accordance with PAIA before a decision is made.

The third party may be afforded an opportunity to make representations as to whether access should be granted or refused. The Information Officer will consider any representations received, together with the requirements of PAIA, before deciding whether to grant or refuse access to the requested record.

10.4 Grounds for refusal of access to records

Ascent may refuse access to a record on any ground permitted or required by PAIA or any other applicable law. A request may be refused where disclosure would result in the unreasonable disclosure of personal information of a third party who is a natural person, including a deceased person, or where the information is otherwise protected under POPIA.

Access may also be refused where the record contains commercial information of Ascent or a third party. This may include trade secrets, financial, commercial, scientific or technical information, information supplied in confidence, intellectual property, methodologies, templates, software, source files, learning content, multimedia content, course material, scripts, storyboards, proposals, pricing models, project methods, business strategies, or any other information which, if disclosed, could reasonably be expected to cause harm to commercial or financial interests or place Ascent or a third party at a disadvantage in negotiations or commercial competition.

Ascent may further refuse access where disclosure would constitute a breach of a duty of confidence owed to a third party, compromise legally privileged information, endanger the life or physical safety of an individual, prejudice the protection of property, or compromise security arrangements, access control measures, systems, premises, facilities, networks, or other protective measures.

Access may also be refused where disclosure would reveal research information of Ascent or a third party, and such disclosure would be likely to expose the identity of the researcher, reveal the subject matter of the research, or place the research at a serious disadvantage.

A request may further be refused if it is manifestly frivolous or vexatious, or if the work involved in processing the request would substantially and unreasonably divert the resources of Ascent. Where only part of a record may lawfully be disclosed, Ascent may grant access to the portion that may be disclosed and refuse access to the remaining portion, where permitted or required by PAIA.

10.5 Fees

A requester may be required to pay the prescribed request fee, access fee, reproduction fee, search and preparation fee, or any other applicable fee provided for under PAIA and its regulations.

The Information Officer may require payment of the prescribed request fee before further processing a request, except where the requester is exempt from paying such fee. Where the preparation of a record exceeds the prescribed number of hours, Ascent may require the requester to pay a deposit before proceeding with the request.

Access to a record may be withheld until all applicable fees have been paid. The prescribed fees payable in respect of requests for access to records are set out in **Annexure B: Prescribed Fees** to this Manual.

10.6 Decision on request

Ascent will consider and decide on a request for access to records as soon as reasonably possible, but in any event within 30 calendar days after receipt of the request, or after receipt of any further particulars required to process the request.

The requester will be notified whether the request has been granted or refused. If access is granted, the requester will be informed of the form in which access will be provided and any applicable fees payable before access is given. If access is refused, the requester will be provided with reasons for the refusal, where required by PAIA, and will be informed of the remedies available to them.

The 30-calendar-day period may be extended once for a further period of not more than 30 calendar days, where permitted by PAIA. This may apply where the request relates to a large number of records, requires searching a large number of records, requires consultation with another party, or cannot reasonably be completed within the original period.

Where an extension is required, the organisation will notify the requester of the extension, the period of extension, and the reasons for the extension.

10.7 Remedies available if access is refused

Ascent does not have an internal appeal procedure. The Information Officer's decision is therefore final within Ascent.

A requester who is dissatisfied with the Information Officer's decision may lodge a complaint with the Information Regulator or apply to a court for appropriate relief, as provided for in PAIA.

10.8 Records not found or not in existence

If all reasonable steps have been taken to locate a requested record and the record cannot be found or does not exist, Ascent will notify the requester accordingly in the manner required by PAIA. Such notification will be regarded as a decision to refuse access to the requested record for purposes of PAIA.

If the record is later found, the requester may be given access to the record, unless access is refused on a ground permitted or required by PAIA.

1. Availability of the Manual

A copy of this Manual is available:

11.1 on Ascent's website, where applicable;

11.2 at Ascent's head office for public inspection during normal business hours;

11.3 to any person upon request, subject to the payment of any prescribed fee, where applicable; and

11.4 to the Information Regulator upon request.

Where a copy of this Manual is requested in printed form, the prescribed fee for reproduction may be payable in accordance with PAIA and its regulations.

2. Updating of the Manual

Ascent will review and update this Manual on a regular basis, or when there are material changes to its operations, contact details, processing activities, records, applicable legislation, or regulatory requirements.

Annexure A – Form 2: Request for Access to Record (Regulation 7)

NOTE:

- Proof of identity must be attached by the requester.
- If requests are made on behalf of another person, proof of such authorisation must be attached to this form.

TO: The Information Officer

(Insert address)

_____

_____

_____

_____

_____

Email address: _____

Fax number: _____

Mark with 'x':

☐ Request is made in my own name. ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full names:				
Identity number:				
Capacity in which request is made (when made on behalf of another person):				
Postal address:				
Street address:				
Email address:				
Contact numbers:	**Tel. (B):**		**Facsimile:**	

	Cellular:	
Full names of person on whose behalf request is made (if applicable):		
Identity number:		
Postal address:		
PARTICULARS OF RECORD REQUESTED Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed).		
Description of record or relevant part of the record:		
Reference number, if available:		
Any further particulars of record:		
TYPE OF RECORD **(Mark the applicable box with an "X")**		
Record is in written or printed form		
The record comprises virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)		

The record consists of recorded words or information which can be reproduced in sound	
The record is held on a computer or in an electronic, or machine-readable form	
MANNER OF ACCESS (Mark the applicable box with an "X")	
Personal inspection of record at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (including transcriptions)	
E-mail of information (including soundtracks if possible)	
Cloud share/file transfer	
Preferred language (Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)	
FORM OF ACCESS (Mark the applicable box with an "X")	
Printed copy of record (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)	
Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)	
Transcription of soundtrack (written or printed document)	
Copy of record on flash drive (including virtual images and soundtracks)	
Copy of record on compact disc drive (including virtual images and soundtracks)	
Copy of record saved on cloud storage server	
PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.	
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:	
FEES: *a)* A request fee must be paid before the request is considered. *b)* You will be notified of the amount of the access fee to be paid. *c)* The fee payable for access to a record depends on the form in which access is required, and the reasonable time required to search for and prepare a record. *d)* If you qualify for exemption of the payment of any fee, please state the reason for exemption.	
Reason:	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication *(Please specify)*

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of requester / person on whose behalf request is made

FOR OFFICIAL USE

Reference number:	
Request received by: (State rank; name and surname of Information Officer)	
Date received:	
Access fees:	
Deposit (if any):	

Signature of Information Officer

Annexure B: Prescribed Fees

The table below sets out the prescribed fees that may be payable when requesting access to records in terms of PAIA. Applicable fees must be paid before access to a record is provided, unless the requester is exempt from payment in terms of PAIA or its regulations.

Item	Description	Amount
1	Request fee, payable by every requester	R140.00
2	Photocopy or printed black and white copy for every A4 page	R2.00 per page or part of the page
3	Printed copy of A4-size page	R2.00 per page or part of the page
4	For a copy in a computer-readable form on: • a flash drive (provided by the requester) • a compact disc (CD) if the requester provides the CD to us • a compact disc (CD) if we give the CD to the requester	R40.00 R40.00 R40.00
5	For a transcription of visual images, for an A4-size page or part of the page	This service will be outsourced. The fee will depend on the quotation from the service provider.
6	For a copy of visual images	This service will be outsourced. The fee will depend on the quotation from the service provider.
7	For a transcription of an audio record, per A4-size page	R24.00
8	For a copy of an audio record on a flash drive (provided by the requester) For a copy of an audio record on compact disc (CD) if the requester provides the CD to us For a copy of an audio record on compact disc (CD) if we give the CD to the requester	R40.00 R40.00 R40.00
9	For each hour or part of an hour (excluding the first hour) reasonably required to search for, and prepare the record for disclosure The search and preparation fee cannot exceed	R145.00 R435.00
10	Deposit: if the search exceeds 6 hours	One-third of the amount per request. It is calculated in terms of items 2 to 8 above.
11	Postage, email or any other electronic transfer	Actual expense, if any.

AST-LG-PAIA-01 PAIA Manual (V5) English

Final Audit Report 2026-06-03

Created:	2026-06-03
By:	Joelene Braun (joelene.braun@ascent.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAA3m_SBQTCjmwRVKDL32_WTZGdfw0xiLvL

"AST-LG-PAIA-01 PAIA Manual (V5) English" History

Document created by Joelene Braun (joelene.braun@ascent.co.za)
2026-06-03 - 1:30:10 PM GMT

Document emailed to Johan Lamberts (johan.lamberts@ascent.tech) for signature
2026-06-03 - 1:30:16 PM GMT

Email viewed by Johan Lamberts (johan.lamberts@ascent.tech)
2026-06-03 - 2:39:04 PM GMT

Document e-signed by Johan Lamberts (johan.lamberts@ascent.tech)
Signature Date: 2026-06-03 - 2:40:29 PM GMT - Time Source: server - Signature Appearance Selected: IMAGE

Agreement completed.
2026-06-03 - 2:40:29 PM GMT