

PAIA Manual

Vorynix Systems

Prepared in accordance with section 51 of the Promotion of Access to Information Act 2 of 2000, as amended, and incorporating applicable requirements of the Protection of Personal Information Act 4 of 2013.

Responsible entity: AgriX Systems (Pty) Ltd

Trading division: Vorynix Systems

Registration number: 2026 / 244372 / 07

Effective date: 12 July 2026

Last updated: 12 July 2026

Version: 1.0

1. Definitions and abbreviations

For purposes of this Manual:

Data subject: The person to whom personal information relates.

Information Officer: The person responsible for PAIA and POPIA compliance within the private body.

Manual: This PAIA Manual.

PAIA: Promotion of Access to Information Act 2 of 2000.

Personal information: Information relating to an identifiable living natural person or, where applicable, an identifiable juristic person.

POPIA: Protection of Personal Information Act 4 of 2013.

Private body: AgriX Systems (Pty) Ltd, operating through Vorynix Systems.

Record: Recorded information held by or under the control of the private body, regardless of its form.

Regulator: Information Regulator of South Africa.

Requester: A person requesting access to a record under PAIA.

Vorynix: Vorynix Systems, the software and systems-development division of the responsible entity.

2. Introduction

The Constitution of the Republic of South Africa recognises the right of access to information.

PAIA gives effect to this right and provides a process through which a person may request access to information held by a public or private body.

A requester seeking information from a private body must generally show that the requested record is required for the exercise or protection of a right, comply with the procedural requirements of PAIA and ensure that no lawful ground for refusal applies.

This Manual describes:

- the identity and contact details of the private body;
- the records held by the private body;
- records that may be publicly available without a formal PAIA request;
- the process for requesting access to records;
- the processing of personal information;
- recipients of personal information;
- possible cross-border data flows;
- general information-security safeguards; and
- the availability and updating of this Manual.

3. Purpose of this Manual

This Manual is intended to assist members of the public to:

- understand the nature and categories of records held by Vorynix;
- identify records that are publicly available without a formal request;
- understand which records may be retained under other legislation;
- obtain the contact details of the Information Officer;
- understand how to submit a request for access to a record;
- understand the fees and procedures that may apply;
- understand how Vorynix processes personal information;
- identify the categories of persons whose personal information may be processed;
- understand how personal information may be shared or transferred;
- understand the general security measures applied by Vorynix; and
- identify the remedies available if a PAIA request is refused or not answered.

4. Details of the private body

Registered entity: AgriX Systems (Pty) Ltd

Trading division: Vorynix Systems

Legal status: South African private company

Registration number: 2026 / 244372 / 07

Country of registration: Republic of South Africa

Registered address: Johannesburg, Gauteng, South Africa

Principal business address: Johannesburg, Gauteng, South Africa

Address for legal service: Johannesburg, Gauteng, South Africa

Website: vorynixsystems.co.za

General enquiries: projects@vorynixsystems.co.za

Direct founder and executive communication: nduvho@vorynixsystems.co.za

Privacy requests: privacy@vorynixsystems.co.za

Information Officer and PAIA requests: informationofficer@vorynixsystems.co.za

Telephone: +27 69 751 8804

4.1 Nature of the business

Vorynix Systems provides services that may include:

- website design and development;
- mobile application development;
- custom business platforms;
- cloud and backend engineering;
- API development and integration;
- artificial-intelligence integration;
- automation systems;
- connected-device and IoT development;
- prototypes and minimum viable products;
- technical consultation;
- system deployment;
- maintenance and support.

5. Information Officer details

Information Officer: Nduvho Silas Mudziwa

Position: Founder and Director

Email: informationofficer@vorynixsystems.co.za

Privacy requests: privacy@vorynixsystems.co.za

PAIA requests: informationofficer@vorynixsystems.co.za

Telephone: +27 69 751 8804

Physical address: Johannesburg, Gauteng, South Africa

Registration status: Active public contact channel

The Information Officer is responsible for facilitating PAIA requests and supporting the body's compliance with PAIA and POPIA.

6. Guide on how to use PAIA

The Information Regulator has published a Guide explaining:

- the objectives of PAIA;
- how to make a request for access to a record;
- assistance available from Information Officers;
- the fees that may apply;
- the grounds on which access may be refused;
- available complaints and court remedies; and
- the prescribed forms used under PAIA.

The Guide is available from the Information Regulator and may also be requested from the Vorynix Information Officer. The Regulator provides the Guide in multiple official South African languages.

7. Records available without a formal PAIA request

The following information may be available publicly without requiring a formal PAIA request:

- Website information, including public website pages, service descriptions and contact details.
- Company information, including public company profile, trading name and service information.
- Portfolio information, including published projects, case studies and project summaries.
- Legal documents, including Privacy Policy, Cookie Policy, Website Terms of Use and Service Terms.
- PAIA information, including this Manual and prescribed request information.
- Marketing material, including public brochures, presentations and promotional content.
- Public announcements, including public notices, news or company updates.
- Vacancies, including publicly advertised employment or contracting opportunities.
- Compliance contacts, including privacy, Information Officer and PAIA contact channels.

Access may be provided through the Vorynix website, email, downloadable electronic documents or another reasonable method determined by the Information Officer.

A record being listed in this section does not require Vorynix to disclose confidential, personal, security-sensitive or legally protected information.

8. Records retained under other legislation

Vorynix may hold records under legislation applicable to its structure and operations.

Depending on the nature of the record and the company's activities, relevant legislation may include:

- Companies Act 71 of 2008;
- Income Tax Act 58 of 1962;
- Tax Administration Act 28 of 2011;
- Value-Added Tax Act 89 of 1991, where applicable;
- Basic Conditions of Employment Act 75 of 1997;
- Labour Relations Act 66 of 1995;
- Employment Equity Act 55 of 1998, where applicable;
- Unemployment Insurance Act 63 of 2001;
- Compensation for Occupational Injuries and Diseases Act 130 of 1993;
- Consumer Protection Act 68 of 2008;
- Electronic Communications and Transactions Act 25 of 2002;

- Protection of Personal Information Act 4 of 2013;
- Promotion of Access to Information Act 2 of 2000;
- Copyright Act 98 of 1978;
- Cybercrimes Act 19 of 2020; and
- any other legislation applicable to a particular project, client, employee, supplier or business activity.

The inclusion of legislation in this Manual does not mean that every record held under that legislation is automatically available.

Access remains subject to applicable confidentiality, privacy, privilege, security and statutory restrictions.

9. Subjects and categories of records held

9.1 Corporate and governance records

Registration and incorporation documents, Memorandum of Incorporation, director and shareholder records, company resolutions, statutory registers, organisational structures, business policies, company ownership records and internal governance documents.

9.2 Financial and accounting records

Quotations and proposals, invoices and payment records, bank and transaction records, accounting records, budgets and forecasts, expense records, tax records and submissions, financial statements, asset records and insurance information.

9.3 Client and project records

Project enquiries, client contact information, consultation records, accepted quotations, contracts and project agreements, scope-of-work documents, project requirements, meeting records, milestone approvals, change requests, support requests, project correspondence, delivery and handover records.

9.4 Software and technical records

System requirements, source code, software repositories, architecture documents, database structures, API specifications, deployment configurations, infrastructure records, access-control configurations, technical documentation, system logs, testing records, incident records, backup and recovery records.

9.5 Intellectual-property records

Trademarks and branding, copyrighted material, software licences, proprietary tools, development frameworks, reusable components, product concepts, design material, invention and prototype records and confidentiality agreements.

9.6 Supplier and contractor records

Supplier contact details, quotations and invoices, service agreements, contractor agreements, confidentiality undertakings, procurement records, due-diligence

information and supplier performance records.

9.7 Personnel and recruitment records

Where applicable: employment applications, curricula vitae, identification and contact details, employment contracts, contractor records, payroll information, performance records, training records, leave records, disciplinary records and health and safety records.

9.8 Marketing and communications records

Website content, social-media content, marketing plans, campaign material, business-development records, portfolio permissions, photographs and media, brand assets, event records and public presentations.

9.9 Privacy and compliance records

Privacy requests, PAIA requests, proof of identity and authority, Information Officer records, data-processing inventories, consent records, objections and corrections, security-compromise records, privacy assessments, operator agreements, regulatory correspondence and compliance training records.

9.10 Security records

Authentication and access records, audit logs, security alerts, incident reports, vulnerability reports, access reviews, firewall or infrastructure records, credential-management records, business-continuity and recovery information.

Detailed security records will ordinarily be restricted where disclosure could compromise systems, users, clients or third parties.

10. Procedure for requesting access to a record

A person requesting access to a record must complete the prescribed Form 2: Request for Access to Record.

The form must be sent to:

- **Information Officer: Vorynix Systems**
- **Email: informationofficer@vorynixsystems.co.za**
- **Address: Johannesburg, Gauteng, South Africa**

The requester must provide sufficient information to enable the Information Officer to:

- identify the requester;
- identify the requested record;
- understand the preferred form of access;
- determine the right the requester seeks to exercise or protect;
- understand why the record is required for that right;
- communicate with the requester; and
- verify any representative authority.

Where a request is submitted on behalf of another person, proof of authority must

accompany the request. Appropriate proof of identity may also be required.

Submitting a request does not guarantee that access will be granted.

11. Fees

A requester may be required to pay the prescribed PAIA request or access fees.

Where applicable, the Information Officer will notify the requester of the amount payable, how the amount was calculated, the method of payment, any deposit required and the right to challenge the fee.

The request may be processed after the prescribed request fee has been paid, where a fee is legally applicable.

The Information Officer will use prescribed Form 3 to communicate the outcome of the request and any applicable fees.

12. Decision on a request

The Information Officer will respond as soon as reasonably possible and ordinarily within 30 calendar days after receiving a complete request.

The period may be extended once for a further period of up to 30 days where permitted under PAIA, including where the request concerns a large number of records, consultation with another party is necessary, the records are not readily available, the requester agrees to an extension, or processing the request within the initial period would unreasonably interfere with operations.

The requester will be informed of an extension and the reasons for it.

The decision may grant access in full, grant partial access, refuse access, or confirm that the requested record cannot be found or does not exist.

13. Grounds for refusing access

Access may be refused where PAIA or another applicable law permits or requires refusal.

Possible grounds include:

- unreasonable disclosure of a third party's personal information;
- disclosure of confidential commercial information;
- disclosure of trade secrets;
- breach of a duty of confidence owed to a third party;
- endangerment of an individual's life or physical safety;
- compromise of system or infrastructure security;
- disclosure of legally privileged information;
- disclosure prohibited by another law;
- prejudice to negotiations or commercial activities;
- disclosure of protected research information;

- records created solely for legal proceedings;
- frivolous or vexatious requests; or
- substantial and unreasonable diversion of resources, where legally applicable.

Where reasonably possible, Vorynix may provide access to a severed or redacted version of a record rather than refusing the entire record.

14. Remedies where a request is refused

A private body does not ordinarily have an internal PAIA appeal procedure.

A requester or affected third party may, subject to PAIA, submit a complaint to the Information Regulator using the prescribed complaint process or approach a competent court.

A complaint may also be submitted where no decision is received within the applicable period, access is refused, an unreasonable fee is charged, access is provided in an unacceptable form, or another PAIA procedural requirement is not followed.

Processing of personal information

15. Purposes for processing personal information

Vorynix may process personal information for purposes including:

- responding to enquiries;
- assessing prospective projects;
- preparing quotations and proposals;
- entering into and administering contracts;
- delivering software and technical services;
- managing client relationships;
- providing support and maintenance;
- processing payments and accounting records;
- managing suppliers and contractors;
- recruitment and personnel administration;
- website security and operation;
- fraud and abuse prevention;
- legal and regulatory compliance;
- record keeping;
- marketing where permitted;
- protecting legal rights;
- managing privacy and PAIA requests;
- investigating security incidents;
- improving services and internal operations.

16. Categories of data subjects and information

Vorynix may process personal information relating to prospective clients, clients, website visitors, client-system users, suppliers and contractors, employees and applicants, business contacts, representatives, information requesters, regulators and advisers.

Information may include names, contact details, company information, project requirements, communications, contractual information, project records, payment records, support information, IP addresses, browser details, device information, form submissions, cookie choices, user identifiers, roles, permissions, technical activity, supplier records, employment information, proof of identity, authority, request information and supporting documents.

Vorynix will process only information that is reasonably necessary and appropriate for the applicable purpose.

17. Recipients of personal information

Personal information may be supplied to employees and authorised representatives, contractors and technical specialists, hosting and cloud-service providers, email and communications providers, payment and accounting service providers, authentication and security providers, analytics providers where enabled, professional advisers, auditors and accountants, insurers, regulators and government bodies, law-enforcement authorities, courts and tribunals, parties involved in a business transfer or restructuring where lawful, and clients where Vorynix acts as an operator on their instructions.

Information will not be sold to third parties.

18. Cross-border processing

Some cloud, infrastructure, communication, software or artificial-intelligence providers may process or store information outside South Africa.

Where cross-border processing occurs, Vorynix will take reasonable steps to ensure that the transfer is lawful, the recipient is subject to appropriate protection, contractual or technical safeguards are applied where necessary, only information required for the relevant service is transferred, and access remains appropriately restricted.

Further details may be provided in the Vorynix Privacy Policy or applicable project agreement.

19. Information-security measures

Vorynix applies reasonable technical and organisational safeguards appropriate to its operations.

These may include encrypted connections, secure website protocols, access controls,

authentication, multifactor authentication where available, restricted administrative permissions, role-based access, secure cloud infrastructure, database access rules, input validation, logging and monitoring, backups, credential management, anti-spam and form-protection measures, software updates, incident-response procedures, confidentiality obligations, contractor access controls and periodic access reviews. Security controls may differ depending on the nature, sensitivity and location of the information concerned.

No system can be guaranteed to be entirely free from risk.

Security, privacy and security-compromise concerns may be reported to privacy@vorynixsystems.co.za.

20. Availability of this Manual

This Manual will be available on the Vorynix Systems website, from the Information Officer upon request, for inspection at the private body's confirmed business address during reasonable business hours, and through any other method required by applicable law.

Electronic copies will ordinarily be made available free of charge.

A prescribed fee may apply where a person requests printed copies or physical reproduction of the Manual.

21. Updating this Manual

The Information Officer will review and update this Manual when necessary, including where company details change, contact information changes, record categories change, processing activities change, service providers change, legislation or regulatory guidance changes, new cross-border processing occurs, or security measures materially change.

The latest version will display its effective date, last-updated date and version number.