POPIA & PAIA **Manual**

ENTRYPRO
security systems

PROTECTION OF PERSONAL INFORMATION ACT (POPIA) COMPLIANCE POLICY & PROMOTION OF ACCESS TO INFORMATION (PAIA) MANUAL

POPIA

1. INTRODUCTION

1.1 Everyone is afforded the right to privacy in terms of section 14 of the Constitution of the Republic of South Africa, 1996 and the Protection of Personal Information Act, 4 of 2013 ("POPIA").

1.2 Through the provision of services, the Company is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

1.3 A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

1.4 Given the importance of privacy, the Company is committed to effectively manage personal information in accordance with the provisions of the POPIA.

1.5 The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information; and in order to –

1.5.1 Regulate, in harmony with international standards, the processing of the personal information of visitors, by the Estate/Complex management and security, in a manner that gives effect to the right to privacy of visitors, subject to justifiable limitations that are aimed at protecting the rights and interests of residents and the Estate/Complex management.

2. DEFINITIONS

2.1. Definitions:

2.1.1. "biometrics" means a technique of personal identification that is based on the physical, physiological or behavioural characterisation including blood typing, fingerprinting, facial recognition, DNA analysis, retinal scanning and voice recognition, as set out in section 1 of the POPIA.

2.1.2. "child" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning himself/herself, as set out in section 1 of the POPIA.

2.1.3. "Company" means Entry Pro (Pty) Ltd, who is a Service Provider in conjunction with others (its operators being the service providers and/or sub-contractors for Entry Pro (Pty) Ltd), and who is a responsible party in certain respects, as defined below, and who is also an operator in other respects, as defined below.

2.1.4. "consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information, as set out in section 1 of the POPIA.

2.1.5. "data subject" means the person to whom personal information relates, as set out in section 1 of the POPIA. For purposes of this policy manual "Data Subject" will relate to the Estate/Complex management, as defined below, and all persons related to the Estate/Complex management.

2.1.6. "Estate/Complex management" means the Estate/Complex management and all persons related to the Estate/Complex management, including but not limited to residents, members, visitors, employees, sub-contractors, operators, service providers, entities, bodies, individuals, companies etc., who is a data subject in certain respects, as defined above, and who is also a responsible party in other respects, as defined below.

2.1.7. "electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient, as set out in section 1 of the POPIA.

2.1.8. "filing system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria, as set out in section 1 of the POPIA.

2.1.9. "information officer" of, or in relation to, a-

(a) public body means an information officer or deputy information officer as contemplated in

terms of section 1 or 17 of the POPIA;
(b) private body means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act, as set out in section 1 of the POPIA.

2.1.10. "Information Regulator" means the Information Regulator established in terms of section 39 of the POPIA, as set out in section 1 of the POPIA.

2.1.11. "Main Agreement" means the Rental Agreement and Service Level Agreement entered into between the Parties.

2.1.12. "operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party, as set out in section 1 of the POPIA, and will include all sub-contractors and service providers of both the Company and the Estate/Complex management.

2.1.13. "PAIA" means the Promotion Of Access To Information Act 2 of 2000, as amended.

2.1.14. "Parties" means the parties to agreements being the Company and the Estate/Complex management.

2.1.15. "person" means a natural person or a juristic person, as set out in section 1 of the POPIA.

2.1.16. "personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-
(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person, as set out in section 1 of the POPIA.

2.1.17. "POPIA" means the Protection Of Personal Information Act 4 of 2013, as amended.

2.1.18. "processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information, as set out in section 1 of the POPIA.

2.1.19. "record" means any recorded information-
(a) regardless of form or medium, including any of the following:
    (i) writing on any material;
    (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
    (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    (iv) book, map, plan, graph or drawing;
    (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
(b) in the possession or under the control of a responsible party;
(c) whether or not it was created by a responsible party; and
(d) regardless of when it came into existence, as set out in section 1 of the POPIA.

2.1.20. "responsible party" means a private body which, in conjunction with others, determines the purpose of and means for processing personal information, as set out in section 1 of the POPIA.

2.1.21. "third parties" means any person or entity unrelated to either the Company or the Estate/Complex management and/or the Data Subject.

3. POLICY MANUAL PURPOSE

3.1. The purpose of this policy manual is to protect the Company from the compliance risks associated with the protection of personal information which includes:

3.1.1. Breaches of confidentiality. The Company could suffer loss in revenue and reputational damage where it is found that the personal information of Data Subjects has been shared or disclosed inappropriately.

3.1.2. Failing to offer choice. All Data Subjects should be free to choose how and for what purpose the Company uses information relating to them.

3.1.3. Reputational damage. The Company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting or accessing the personal information held by the Company.

3.2 This policy manual demonstrates the Company's commitment to protecting the privacy rights of Data Subjects in the following manner:

3.2.1 Through stating desired behaviour and directing compliance with the provisions of the POPIA and best practice.

3.2.2 By cultivating a culture that recognises privacy as a valuable human right.

3.2.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

3.2.4 By creating business practices that will provide reasonable assurance that the rights of Data Subjects are protected and balanced with the legitimate business needs of the Company.

3.2.5 By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officer in order to protect the interests of the Company and Data Subjects.

3.2.6 By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

3.3 It is hereby recorded that it is the business of the Company to process personal information of Data Subjects in order to provide the services in terms of the Main Agreement between the Parties, and it is understood that:

3.3.1 Visitors to the estate/complex are "data subjects", as set out in section 1 of the POPIA.

3.3.2 Visitors' information as it appears on their driver's license and vehicle license discs qualifies as "personal information", as set out in section 1 of the POPIA.

3.3.3 The scanning of said personal information qualifies as "processing", as set out in section 1 of the POPIA.

3.3.4 The provision of personal information by the Data Subjects to the Estate/Complex management, the Company and its operators are mandatory in order to gain access to the estate/complex.

3.4 This policy manual further provides for the policies implemented and procedures to be followed in order to access information held by the Company in terms of the PAIA Act.

4 POLICY MANUAL APPLICATION

4.1 This policy manual and its guiding principles apply to:

4.1.1 The Company's directors.

4.1.2 All branches, business units and divisions of the Company.

4.1.3 All employees and volunteers.

4.1.4 All contractors, suppliers and other persons acting on behalf of the Company.

4.1.5 The policy manual's guiding principles find application in all situations and must be read in conjunction with the POPIA as well as the PAIA Act.

4.2 The Company undertakes that:

4.2.1 It recognises its accountability towards visitors and residents of the estate/complex in terms of section 8 of the Act.

4.2.2 Processing of information is done lawfully and in line with the provisions of section 9 of the Act.

4.2.3 Processing is necessary to ensure security of access to the estate/complex in terms of the Main Agreement between the Company and the Estate/Complex management (section 11(1)(b)).

4.2.4 Processing of personal information is done in order to protect a legitimate interest of the Data Subject, residents and Estate/Complex management and will not prejudice a legitimate interest of the Data Subject (section 11(1)(d)).

4.2.5 Processing is necessary for pursuing a legitimate interest of the estate/complex and/or the Estate/Complex management.

4.2.6 Personal information is collected for the specific purpose of ensuring the safety, security and accountability of all visitors, residents and employees of the complex/management.

4.2.7 The Client/Data Subject acknowledges and accepts full responsibility for obtaining all necessary consents from Homeowners, Residents, Tenants, Contractors, Workers, and Visitors to the Estate/Client/Data Subject for the collection, processing, and recording of personal information, as required under the Protection of Personal Information Act, 2013 ("POPIA"). The Company/Service Provider operates on the assumption that the Client/Data Subject has implemented appropriate policies, procedures, protocols, and safeguards to ensure compliance with POPIA and that all required permissions have been duly obtained.

4.2.8 By entering into this Agreement, the Client/Data Subject grants the Company/Service Provider permission to process personal information on its behalf, within the scope of the services rendered. The Company/Service Provider shall not be held liable or responsible in any manner whatsoever for any failure by the Client/Data Subject to obtain the necessary consents or to comply with applicable data protection obligations.

4.2.9 Personal information recorded shall not be used for any purpose other than that set out herein.

4.2.10 Records of personal information provided shall not be retained longer than is necessary for the purpose outlined above (subject to the provisions of section 14).

4.2.11 Failure to provide the personal information required shall lead to access to the premises being denied.

5 RIGHTS OF DATA SUBJECTS

5.1 Where appropriate, the Company will ensure that its clients and customers are made aware of the rights conferred upon them as Data Subjects.

5.2 The Company will ensure that it gives effect to the following rights.

5.2.1 The Right to Access Personal Information.

5.2.1.1 The Company recognises that a Data Subject has the right to establish whether the Company holds personal information related to him, her or it, including the right to request access to that personal information. Any request for information must be dealt with in accordance with the provisions of this PAIA manual.

5.2.2 The Right to have Personal Information Corrected or Deleted

5.2.2.1 The Data Subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the Company is no longer authorised to retain the personal information.

5.2.3 The Right to Object to the Processing of Personal Information

5.2.3.1 The Data Subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

5.2.3.2 In such circumstances, the Company will give due consideration to the request and the requirements of the POPIA.

5.2.3.3 The Company may cease to use or disclose the Data Subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.2.4 The Right to Object to Direct Marketing

5.2.4.1 The Data Subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.2.5 The Right to Complain to the Information Regulator

5.2.5.1 The Data Subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under the POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

5.2.6 The Right to be Informed

5.2.6.1 The Data Subject has the right to be notified that his, her or its personal information is being collected by the Company.

5.2.6.2 The Data Subject also has the right to be notified in any situation where the Company has reasonable grounds to believe that the personal information of the Data Subject has been accessed or acquired by an unauthorised person.

6 GENERAL GUIDING PRINCIPLES

6.1 All employees and persons acting on behalf of the Company will always be subject to, and act in accordance with, the following guiding principles:

6.2 Accountability

6.2.1 Failing to comply with the POPIA could potentially damage the Company's reputation or expose the Company to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

6.2.2 The Company will ensure that the provisions of the POPIA and the guiding principles outlined in this policy manual are complied with through the encouragement of desired behaviour. However, the Company will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy manual.

6.3 Processing Limitation

6.3.1 The Company will ensure that personal information under its control is processed:

6.3.1.1 in a fair, lawful and non-excessive manner; and

6.3.1.2 only with the informed consent of the Data Subject; and

6.3.1.3 only for a specifically defined purpose.

6.3.2 The Company will inform the Data Subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information. By concluding a Main Agreement with the Company, the Estate/Complex management warrants that it has obtained all the necessary consents from its residents, and further acknowledges that the signature of the Main Agreement between the Parties constitutes written consent for purposes of the POPIA.

6.3.3 Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the Company will maintain a voice recording of the stated purpose for collecting the personal information followed by the Data Subject's subsequent consent, in terms of the Main Agreement between the Parties.

6.3.4 The Company will under no circumstances distribute or share personal information between separate legal entities, associated companies (such as subsidiary companies or sub-contractors) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

6.3.5 Where applicable, the Data Subject must be informed of the possibility that their personal information will be shared with other aspects of the Company's business and be provided with the reasons for doing so.

6.4 Purpose Specification

6.4.1 All of the Company's business units and operations must be informed by the principle of transparency.

6.4.2 The Company will process personal information only for specific, explicitly defined and legitimate reasons. The Company will inform Data Subjects of these reasons prior to collecting or recording the Data Subject's personal information.

6.5 Further Processing Limitation

6.5.1 Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

6.5.2 Therefore, where the Company seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the Data Subject.

6.6 Information Quality

6.6.1 The Company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

6.6.2 The more important it is that the personal information be accurate, the greater the effort the Company will put into ensuring its accuracy.

6.6.3 Where personal information is collected or received from third parties, the Company will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the Data Subject or by way of independent sources.

6.7 Open Communication

6.7.1 The Company will take reasonable steps to ensure that Data Subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

6.7.2 The Company will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for Data Subjects who want to:

6.7.2.1 Enquire whether the Company holds related personal information, or
6.7.2.2 Request access to related personal information, or
6.7.2.3 Request the Company to update or correct related personal information, or
6.7.2.4 Make a complaint concerning the processing of personal information.

6.8 Security Safeguards

6.8.1 The Company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

6.8.2 Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, the greater the security required.

6.8.3 The Company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company's IT network.

6.8.4 The Company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

6.8.5 All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the Company is responsible.

6.8.6 All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contract containing the relevant consent and confidentiality clauses.

6.8.7 The Company's operators and sub-contractor service providers will be required to enter into service level agreements with the Company where both parties pledge their mutual Protection of Personal Information policy manual commitment to the POPIA and the lawful processing of any personal information pursuant to the agreement.

6.8.8 Security compromises that meet the threshold for reporting must be reported to the Information Regulator using the Regulator's e-Services Portal. The Information Officer must submit an initial report within the internal SLA of 72 hours of becoming aware (should it be deemed necessary) and must include the facts of the compromise, categories of personal information affected, likely consequences, and mitigation steps.

6.8.9 Security Compromise and Breach Reporting

6.8.9.1 Scope and threshold - A security compromise (breach) is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information processed by or on behalf of the Company. Where the Company has reasonable grounds to believe a security compromise has occurred, the incident must be treated as reportable.

6.8.9.2 Internal escalation - Any employee, contractor or operator who becomes aware of a suspected or confirmed security compromise must immediately notify the Information Officer and the IT Service Provider. The Information Officer must be notified **without delay** and an initial internal incident record must be created within **24 hours** of detection.

6.8.9.3 Information Regulator reporting - Where the incident meets the statutory threshold for reporting under POPIA, the Information Officer must submit a report to the **Information Regulator using the Regulator's e-Services Portal**. An initial report to the Regulator must be submitted within **72 hours** of the Information Officer becoming aware that the incident meets the reporting threshold, unless a shorter statutory period applies. The report must include, at minimum: the nature of the compromise; categories of personal information affected; estimated number of data subjects affected; likely consequences; measures taken or proposed to mitigate harm; and contact details for the Company's Information Officer.

6.8.9.4 Interim communications and remediation - The Information Officer will coordinate interim communications to affected Data Subjects and the Estate/Complex management where required, and will document all mitigation steps, forensic findings and remedial actions. All communications must be approved by the Information Officer prior to release.

6.8.9.5 Recordkeeping and review – A post-incident report and lessons-learned review must be completed within 30 days of incident closure and retained for audit purposes.

6.9 Data Subject Participation

6.9.1 A Data Subject may request the correction or deletion of his, her or its personal information held by the Company.

6.9.2 The Company will ensure that it provides a facility for Data Subjects who want to request the correction or deletion of their personal information.

6.9.3 Where applicable, the Company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7 CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

7.1 The Company processes personal information relating to residents, visitors, contractors, service providers, employees and other data subjects in South Africa and Botswana.

7.2 In the course of providing cloud-based access control, visitor management, estate security and related services, personal information may be stored, processed, transmitted, backed up or accessed outside the Republic of South Africa.

7.3 The Company's primary cloud infrastructure and certain supporting technology services are hosted in the United States of America. As a result, personal information collected in South Africa or Botswana may be transferred to, stored in, or processed in the United States and other jurisdictions where the Company's authorised service providers operate.

7.4 The Company will only transfer personal information outside South Africa where such transfer complies with section 72 of the Protection of Personal Information Act, 4 of 2013 ("POPIA"), including where:

7.4.1 The recipient is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection substantially similar to the requirements of POPIA;

7.4.2 The transfer is necessary for the performance of a contract or service requested by the data subject or the Company's client;

7.4.3 The data subject has consented to the transfer where consent is required; or

7.4.4 Another lawful ground for transfer exists in terms of POPIA.

7.5 The Company requires all third-party operators, cloud hosting providers, infrastructure providers and sub-processors that process personal information on its behalf to implement appropriate technical and organisational security measures, including measures designed to prevent unauthorised access, disclosure, alteration, loss or destruction of personal information.

7.6 Where personal information originating from Botswana is processed, the Company will additionally comply with all applicable requirements of Botswana's data protection legislation relating to international data transfers.

7.7 The Company maintains written agreements with relevant operators and service providers governing the processing, confidentiality, security and protection of personal information transferred across borders.

7.8 The Company remains accountable for personal information under its control and takes reasonable steps to ensure that any foreign recipient processes such information in accordance with applicable data protection laws and contractual safeguards.

8 INFORMATION OFFICERS

8.1 The Company has appointed an Information Officer and a Deputy Information Officer to assist the Information Officer.

8.2 The Company’s Information Officer responsibilities and registration:

8.2.1 Registration – The Company’s Information Officer must be registered with the South African Information Regulator and must maintain an active account for the Regulator’s e-Services Portal. The Information Officer shall provide the Information Regulator registration reference and the date of registration to the Company and update this information in the manual whenever it changes.

8.2.2 Primary duties – The Information Officer is the Company’s primary contact for all POPIA and PAIA matters and is responsible for: maintaining this POPI & PAIA manual; receiving and responding to Data-Subject requests; coordinating breach reporting to the Information Regulator; ensuring that operators and sub-contractors have appropriate POPIA safeguards; maintaining records of processing activities; and providing periodic compliance reports to the Governing Body.

8.2.3 Delegation and availability – The Information Officer may delegate operational tasks to the Deputy Information Officer or other authorised staff but remains accountable for compliance. The Information Officer must ensure that the Regulator’s portal contact details are current and that an alternate contact (Deputy Information Officer) is available during absences.

8.3 Once appointed, the Company will register the Information Officer with the South African Information Regulator established under the POPIA prior to performing his or her duties.

8.4 Should you require further information, please contact the Company:

New Company Name	**Entry Pro (Pty) Ltd**

Address	Solutions House, 42 Gazelle Close, Corporate Park South, Midrand, 1685
Postal Address	PO Box 6735, Halfway House, Johannesburg, 1685
Telephone	011 267 0720
Fax	0866010299
Email	elize@entrypro.co.za
Information Officer	Dave Adams
Deputy Information Officer	Elize Van der Merwe
Information Regulator registration number	2025-059880

9 SPECIFIC DUTIES AND RESPONSIBILITIES

9.1 Governing Body

9.2 Information Officer

9.3 IT Service Provider

9.4 Marketing & Communication Manager

9.5 Employees and other persons acting on behalf of the Company

9.6 Data security and encryption.

9.6.1 Data stored by the Company is encrypted and hosted on secure servers, provided by operators.

9.6.2 Accessing the data is by secure login to an encrypted site.

9.6.3 All users are required to register with the Company before being given access.

9.6.4 It is the Estate/Complex management's responsibility to ensure that users are POPI compliant and have the necessary authority levels to gain access.

9.6.5 All user details are secured, and only specific users can access the Company's data.

9.6.6 All user credentials are kept under their specific estate/complex.

9.6.7 Passwords policy aligned to current best practice; MFA; patching SLA; logging and retention.

9.6.8 Data storage is also conducted cross-border with all safeguards in place.

9.7 Firewall Protection and Anti-virus/Malware Protection:

9.7.1 Firewall Protection:

9.7.1.1 The firewall is configured to only allow connections from specific ports. Upgrades are done on communicated releases, once the Company have been notified of a change, the Company schedule the upgrade to take place.

9.7.1.2 The database will only accept connections from the application which is designed to prevent SQL (structured query language) injection attacks.

9.7.1.3 All devices that connect to the system (Scanners etc) have to be registered on the system first otherwise the connection is rejected. The system uses secure tokens to determine if access should be allowed.

9.7.1.4 All communication is done via HTTPS using a secure signed certificate.

9.7.2 Antivirus/Malware Protection:

9.7.2.1 The antivirus and malware application are configured for live updates. As soon as the service provider releases an update it automatically installs at night without down time. The antivirus monitors all incoming connections and blocks anything that is determined as unsafe. Scans are done every day at 01h00 in the morning.

9.7.2.2 The operating system updates are done every month unless there is an urgent security patch released, in which case the update is scheduled as soon as possible.

10 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

10.1 Data Subjects have the right to:

10.1.1 Request what personal information the Company holds about them and why.

10.1.2 Request access to their personal information.

10.1.3 Be informed how to keep their personal information up to date.

10.2 Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the Data Subject with a "Personal Information Request Form".

10.3 Once the completed form has been received, the Information Officer will verify the identity of the Data Subject prior to handing over any personal information. All requests will be processed and considered against the Company's PAIA policy manual.

10.4 The Information Officer will process all requests within a reasonable time.

10.5 Acknowledgement of Requests (to be sent on receipt of a valid request):

Subject: Acknowledgement of your Personal Information Request

Dear [Name],

We confirm receipt of your request for personal information dated [date]. We will verify your identity and process your request in accordance with the POPIA and this manual. If we require further information to verify your identity or to clarify your request, we will contact you within **72 hours**. We will provide a substantive response within 30 days or notify you of any lawful extension and the reasons for it.

Contact: [Information Officer name, email, telephone].

Yours sincerely,

Information Officer

10.6 Refusal and Appeal Template (to be sent when a request is refused in whole or in part):

Subject: Outcome of your Personal Information Request

Dear [Name],

We refer to your request dated [date]. After consideration, we are unable to provide the requested information for the following reason(s): [set out specific legal grounds, e.g., third-party privacy, privileged information, manifestly unfounded/vexatious request, or other statutory ground].

You have the right to request a review of this decision by the Information Officer within 30 days. If you remain dissatisfied, you may lodge a complaint with the Information Regulator. The Regulator's contact details and complaint procedure are available on its website.

If you would like to request a review or provide further information, please contact [Information Officer name, email, telephone].

Yours sincerely,

Information Officer

10.7 Should you require further information, please contact the Company:

New Company Name	**Entry Pro (Pty) Ltd**
Address	Solutions House, 42 Gazelle Close, Corporate Park South, Midrand, 1685
Postal Address	PO Box 6735, Halfway House, Johannesburg, 1685
Telephone	011 267 0720
Fax	0866010299
Email	elize@entrypro.co.za

11 POPI COMPLAINTS PROCEDURE

11.1 Data Subjects have the right to complain in instances where any of their rights under the POPIA have been infringed upon. The Company takes all complaints very seriously and will address all POPI related complaints in accordance with the procedure set out herein.

12 DISCIPLINARY ACTION

11.1 Where a POPI complaint or a POPI infringement investigation has been finalised, the Company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy manual.

11.2 In the case of ignorance or minor negligence, the Company will undertake to provide further awareness training to the employees.

11.3 Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the Company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

11.3.1 Examples of immediate actions that may be taken subsequent to an investigation include:

11.3.1.1 A recommendation to commence with disciplinary action.

11.3.1.2 A referral to appropriate law enforcement agencies for criminal investigation.

11.3.1.3 Recovery of funds and assets in order to limit any prejudice or damages caused.

13 INTRODUCTION

13.1 The POPI and PAIA Acts provide for certain records and/or information to be accessed where certain circumstances are met and in accordance with certain procedures and at prescribed fees, giving effect to the right of access to information in terms of the Constitution of the Republic of South Africa.

13.2 This POPI and PAIA Manual has been prepared in accordance with section 51 of the PAIA Act as read with the POPIA. (Promotion of Access to Information Act 2 of 2000 – PAIA)

13.3 The Company has appointed an Information Officer in accordance with the POPIA. In addition to its obligations prescribed under the POPIA, the designated Information Officer is also responsible for assessing any requests to the Company for access to information in terms of the PAIA Act as well as to oversee any other obligations which the Company may have under the PAIA Act. The Information Officer has appointed a Deputy Information Officer to assist him in the fulfilment of these obligations.

14 GUIDE ON HOW TO USE PAIA

14.1 The South African Human Rights Commission (SAHRC) has issued a guide on how to use the Act (as prescribed by section 10 of PAIA) and is available on the SAHRC website (www.sahrc.org.za). This Manual complies with the requirements of the guide (defined below) and recognises that the Information Regulator established under POPI will be responsible for regulating compliance with PAIA, POPI and their regulations.

14.2 See contact details below:

PAIA	POPI
South African Human Rights Commission **Promotion of Access to Information Act Unit** **Research and Documentation Department** **Private Bag 2700** **Houghton** **Johannesburg** **2041** **Telephone: +27 11 887 3600** **Email:** paia@sahrc.org.za	Information Regulator **Physical address:** JD House 27 Stiemens Street Braamfontein, Johannesburg 2001 **Postal address:** P.O Box 31533 Braamfontein Johannesburg 2017 **Email:** Complaints: complaints.IR@justice.gov.za General enquiries: inforeg@justice.gov.za.

15 RECORDS HELD BY THE COMPANY

15.1 Records which are freely available (section 51(1)(c) of the PAIA Act)

15.1.1 The following records are automatically available to the general public and need not be requested in accordance with the procedure outlined in this Manual:

- brochures;
- information available on the Company's website.

15.2 Records held by the Company in terms of other legislation (section 51(1)(d) of PAIA) that is not freely available

15.2.1 The Company retains a number of records in accordance with legislation which applies to it, such records may include but are not limited to:

- Basic Conditions of Employment Act No 75 of 1997;

- Companies Act No 71 of 2008;
- Compensation for Occupational Injuries and Diseases Act No 130 of 1993;
- Consumer Protection Act No 68 of 2008;
- Copyright Act No 98 of 1978;
- Electronic Communications and Transactions Act No 25 of 2002;
- Employment Equity Act No 55 of 1998;
- Financial Intelligence Centre Act No 38 of 2001;
- Income Tax Act No 58 of 1962;
- Labour Relations Act No 66 of 1995;
- Medical Schemes Act No 131 of 1998;
- National Credit Act No 34 of 2005;
- Occupational Health and Safety Act No 85 of 1993;
- Pension Funds Act No 24 of 1956;
- Protection of Personal Information Act No 4 of 2013;
- Regulation of Interception of Communications and Provision of Communication-Related Information Act No 70 of 2002;
- Skills Development Act No 97 of 1998;
- Skills Development Levies Act No 9 of 1999;
- Unemployment Insurance Act No 63 of 2001;
- B-BBEE Act No 53 of 2003; and Value Added Tax Act No 89 of 1991.

15.2.2 Where any information contained in any records retained by the Company in terms of the above legislation is of a public nature, such records may be available for inspection without a person having to request access thereto in terms of the PAIA Act.

15.3 Records held by the Company (section 51(1)(e) of the PAIA Act) not freely available

15.3.1 The records held by the Company may include but are not necessarily limited to:

15.3.1.1 Human resources

a) Employee information including personal information, employment history and health records that the Company may hold from time to time;
b) Disciplinary records;
c) Employment equity plan;
d) Records of pension and provident funds;
e) Training and development information;
f) General files containing information on employee benefits and employee recruitment and selection information;
g) List of employees;
h) Employment contracts;
i) Tax records;
j) Training records;
k) Payroll; and
l) Applicable internal policies and procedures.

15.3.1.2 Client-related records (Estate HOA, Residents, Contractors, Visitors for the only purpose of Estate Security)

a) FICA records;
b) Biometric information;
c) Personal Information; and
d) Correspondence.

15.3.1.3 Property

a) Lease agreements;
b) Insurance records; and
c) Asset register.

15.3.1.4 Operations

a) Function records and related costings;
b) Stock sheets;
c) List of suppliers; and
d) Supplier agreements.

15.3.1.5 Information technology

a) Licence agreements;
b) Records relating to systems;

c) Domain information;
d) Usage statistics;
e) Equipment details; and
f) Costings of hardware and software.

15.3.1.6 Company information

a) The Company secretarial records; and
b) Incorporation documents, including Memorandum and Incorporation.

15.3.1.7 Finance/Accounts department

a) Accounting records;
b) Annual financial statements;
c) Tax returns;
d) Creditors and debtors;
e) Invoices;
f) Salary information;
g) Banking records;
h) Bank account details;
i) Fixed assets register;
j) Audit reports.

15.3.1.8 Marketing department

a) The Company brochures and publications;
b) Documents relating to public relations events; and
c) The Company media releases.

16 INTERNATIONAL PROCESSING AND STORAGE OF PERSONAL INFORMATION

16.1 The Company operates a cloud-based technology platform used for access control, visitor management and estate security services.

16.2 Personal information collected and processed by the Company may be stored on systems located outside South Africa, including cloud infrastructure located in the United States of America.

16.3 The Company may transfer personal information across national borders where such transfer is necessary for the provision of its services, system administration, data backup, business continuity, technical support, cybersecurity functions or other legitimate operational purposes.

16.4 All international transfers of personal information are conducted in accordance with the Protection of Personal Information Act, 4 of 2013 ("POPIA"), applicable contractual safeguards and any other applicable data protection legislation.

16.5 The Company takes reasonable measures to ensure that recipients of personal information outside South Africa maintain an adequate level of protection and security for such information.

17 PROCESS FOR REQUESTS TO INFORMATION

17.1 Any requests for access to records of and held by the Company are subject to the PAIA Act and, in respect of personal information, the POPIA.

17.2 In terms of the PAIA Act, a request for access is to be made on the prescribed form which can be requested via email to the Information Officer and Deputy Information Officer. The request is to be made to the Information Officer and Deputy Information Officer addressed to the contact details set out above (section 53(1) of the PAIA Act).

17.3 The requester must provide sufficient detail on the form to enable the Information Officer to identify the record and the requester. The requester should also indicate which form of access is required and specify a postal address and fax number in the Republic of South Africa or email address. The requester should also indicate if, in addition to a written reply, any other manner is to be used to inform the requester and state the necessary particulars to be so informed (section 53(2)(a) and (b) and (c) and (e) of the PAIA Act).

17.4 The requester must identify the right that is sought to be exercised or protected and provide an explanation of why the requested record is required for the exercise or protection of that right (section 53(2)(d) of the PAIA Act).

17.5 In circumstances where the request for access is being made on behalf of another person, the requestor is obliged to prove the capacity in which the request is being made, with any submissions in support thereof being subject to the satisfaction of the Company (section 53(2)(f) of the PAIA Act). Section 71 of the PAIA Act makes provision for a request for information or records about a third party. In considering such a request, the Company will adhere to the provisions of sections 71 to 74 of the PAIA Act. The requestor is to note the provisions of Chapter 5 of Part 3 of the PAIA Act in terms of which the Company is obliged, in certain circumstances, to advise third parties of requests lodged in respect of information applicable to or concerning such third parties. In addition, the provisions of Chapter 2 of Part 4 of the PAIA Act entitle third parties to dispute the decisions of the Company by referring the matter to the High Court.

17.6 The Information Officer will decide on whether or not to grant the request as soon as is reasonably possible (but in any event within thirty (30) days of the request having been submitted) and notify the requester accordingly.

17.7 The Information Officer may decide to extend the period of thirty (30) days for another period of not more than thirty (30) days if:

17.7.1 the request is for a large number of records;

17.7.2 the search for the records is to be conducted at premises not situated in the same town or city as the head office of the Company;

17.7.3 consultation among divisions or departments, as the case may be, of the Company is required;

17.7.4 the requester consents to such an extension in writing; or

17.7.5 the parties agree in any other manner to such an extension.

17.8 Should the Company require an extension of time, the requester shall be informed in the manner stipulated in the prescribed form of the reasons for the extension.

17.9 If the Information Officer fails to respond (or within the extended period within which to respond) within thirty (30) days after a request has been received, it will, in terms of the PAIA Act, be deemed to have refused the request (section 58 read together with section 56(1) of the PAIA Act).

17.10 Where access is granted:

17.10.1 the Information Officer will advise the requester of:

a) the access fee to be paid for the information (in accordance with paragraph 15.11 of this Manual below) prior to the Company being able to process the request and grant the access (section 54(1) of the PAIA Act);

b) the format in which access will be given;

c) the fact that the requester may lodge an appeal with a court of competent jurisdiction against the access fee charged or the format in which access is to be granted (section 56(2) of the PAIA Act); and

17.10.2 access to the record requested will be given as soon as reasonably possible.

17.11 The following access and reproduction fees apply:

17.11.1 the request fee payable by a requester, other than a personal requester (being a requester who seeks access to a record containing personal information about that requester) is R140,00. The requester may lodge an application to the court against the tender or payment of the request fee (section 54(3)(b) of the PAIA Act); and

17.11.2 where the Information Officer is of the opinion that the number of hours required to search, reproduce and/or prepare the information requested will exceed 6 hours, it may require that a deposit be paid, calculated in accordance with the PAIA Act.

17.11.3 Access and Reproduction fees respectively:

For every photocopy of an A4 size page or part thereof	R2.00
For every printed copy of an A4 size page or part thereof	R2.00
For a copy of a compact disc (supplied by requester)	R40.00
For a transcript of visual images for an A4 size page or part thereof	As per quotation from service provider
For a copy of visual images	As per quotation from service provider
For a transcript of an audio record, for an A4 size page or part thereof	R24.00
For a copy of an audio record	R40.00
For a USB drive (supplied by requester)	R40.00
For searching for and obtaining record, charged per hour	R145.00 (minimum) R435.00 (maximum)

17.12 If the request for access is refused, the Information Officer shall advise the requester in writing of the refusal, including adequate reasons for the refusal and that the requester may lodge an appeal with a court of competent jurisdiction against the refusal of the request (section 56(3) of the PAIA Act).

17.13 Upon the refusal by the Information Officer, any deposit paid by the requester will be refunded.

17.14 The requester may lodge an appeal with a court of competent jurisdiction against any process set out in this paragraph.

18 RECORDS NOT FOUND

18.1 If a record cannot be found or if the records do not exist, the Information Officer shall notify the requester (providing full details of steps taken to find the record or determine its existence) that it is not possible to give access to the requested record.

18.2 If the record in question should later be found, the requester shall be given access to the record unless access is refused by the Company.

19 REFUSAL OF ACCESS

19.1 The Company may refuse to grant access on certain grounds, including the following (Part 3, Chapter 4 of the PAIA Act):

19.1.1 that the record constitutes privileged information for the purposes of legal proceedings or is subject to professional privilege and/or confidentiality;

19.1.2 to protect the commercial information or the confidential information of a third party or the Company;

19.1.3 that it is necessary to protect the safety of individuals or property;

19.1.4 that it is necessary to protect the research information of a third party or the Company; or

19.1.5 that granting access would result in the unreasonable disclosure of personal information about a third party.