XSYS South Africa (Pty) Ltd

2021/477264/07

POPI & PAIA MANUAL

FOR THE IMPLEMENTATION OF THE SOUTH AFRICAN
PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013
&
FOR THE APPLICATION OF THE SOUTH AFRICAN
PROMOTION OF ACCESS TO INFORMATION ACT NO. 2 OF 2000 (as amended)

Designed and Compiled by
RANDCO
corporate governance
and company secretarial consultancy

TABLE OF CONTENTS

SCOPE OF THE MANUAL

Nature of Business: Sale of products (printing plates, sleeves, adapters, prepress and processing equipment) for the flexographic printing industry and providing corresponding (technical) services and support.

The scope of the manual is limited to the records held by **XSYS SOUTH AFRICA (PTY) LTD**

COMPANY CONTACT DETAILS

XSYS South Africa (Pty) Ltd
2021/4772264/07
91 Mimetes Road, Denver Ext. 4, Johannesburg, Gauteng, 2094
Tel: (+27) 082-443-7319
Email: gordon.smith@xsysglobal.com
Website: www.xsysglobal.com/privacy-policy

The Information Officer: **Gordon Smith**
Dedicated email address for POPI/PAIA: gordon.smith@xsysglobal.com
Contact numbers: 082 443 7319

1. PURPOSE OF THIS MANUAL

The Protection of Personal Information Act 4 of 2013 (POPIA) and the Protection of Personal Information Act 2 of 2000 (PAIA), gives effect to Section 32 of the Constitution's right of privacy and looks at two opposing interests relating to that of personal information, from an individual point of view and access to personal information for the legitimate purpose of conducting business.

POPIA provides guiding principles to promote the protection of privacy which are intended to be applied to the processes of personal information accessibility and sharing.

PAIA gives legislative effect to person's right of access to information and accountability for both private and public bodies who has a duty to provide to a requester of records, unless specifically refused in terms of Section 11 of PAIA. It's designed to empower people to use the law and empower themselves so as to facilitate the requesting of access of information in different ways.

The purpose of this manual as set out below is to protect **XSYS South Africa (Pty) Ltd** and to inform stakeholders and data subjects of the compliance associated with the protection of, and the right to access, Personal Information which includes:

- breaches of confidentiality;
- failing to offer choice; and
- reputational damage;

This manual is linked to XSYS Global Personal Data Breach Procedure and XSYS Global Personal Data Privacy Policy.

XSYS South Africa (Pty) Ltd will ensure that the highest standard of compliance with policies, regulations, and laws to protect Personal Information is maintained at all times.

2. AVAILABILITY OF THIS MANUAL

a. This PAIA and POPI Manual is available for inspection during office hours from the Information Officer, free of charge, subject to format requested.
b. Additionally, this PAIA and POPI Manual can be viewed on the Company website at: www.xsysglobal/privacy-policy

3. GENERAL DEFINITIONS

Access	The right, the opportunity, or the means of finding, using, or retrieving information
Accountability	The condition that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others
Anonymous	Information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Anonymous information	Information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.
Anti-malware	Software that is designed to identify and prevent malicious software, or malware, from infecting computer systems or electronic devices.
Anti-virus	Software designed to detect and destroy computer viruses.
Automated decision making	Decisions made by machine (computers), without human intervention. For example, to automatically accept or deny an online credit application or the automated processing of CVs that evaluates (profiles) personal aspects of individuals to determine if they will qualify for a position.
Availability	The guarantee of reliable access to information by authorised people
Binding corporate rules	Personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country.
Biometric data	Personal information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Classification	The process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection
Confidentiality	Is managed by the set of rules that limits access to information
Consent	Of the data subject means, any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information
Continuity	Encompasses planning and preparation to ensure that an organisation can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period
Core activities	The core activities of a Responsible Party relate to primary activities and do not relate to the processing of personal information as ancillary activities. An example of an ancillary activity would be a organisation paying the salaries of its workers. However, the core activity of a hospital is to provide health care and it could not provide healthcare safely and effectively without processing health data, such as patients' health records. Those activities cannot be considered ancillary and must be considered as core.
Data mapping	The process used to identify what personal information you use, why you use it, how sensitive it is, how long you may retain it, where you process it and where you collect it.
DPA (Data Processing Agreement)	An agreement between a data controller and a data processor, thereby regulating the processing of data for business purposes.
Data subject	The person to whom personal information relates.

De-identified	Information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.
Disaster recovery	The process or actions for an organisation to minimise the effects of a disruptive incident, to continue to operate or quickly resume mission-critical functions.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access
Filing system:	Any structured set of personal information which are accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis
Health	Personal information related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status
High-risk	Activities including, but not limited to, large scale data processing which could affect a large number of individuals; regular and systematic monitoring; the transfer of personal information to countries which don't have adequate privacy
Integrity	The assurance that information is trustworthy and accurate
International organisation	An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Large-scale data processing	Examples include - patient data in the regular course of business by a hospital; travel data of individuals using a city's public transport system (e.g. tracking via travel cards); real time geo-location data of customers of an international fast food chain for statistical purposes by an Operator specialised in these activities; customer data in the regular course of business by an insurance organisation or a bank; personal information for behavioural advertising by a search engine; data (content, traffic, location) by telephone or internet service providers. Examples that do NOT constitute large-scale processing include - processing of patient data by a single physician; processing of personal information relating to criminal convictions and offences by an individual lawyer.
Operator	A natural or legal person, public authority, agency or other body which processes personal information on behalf of the Responsible Party. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.
Personal information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person such as a company, including, but not limited to. **Personal Information:** Personal information is any information that can be used to reveal a person's identity. • race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;

	• information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; • the biometric information of the person; • the personal opinions, views or preferences of the person; • 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; • the views or opinions of another individual about the person; • 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.
Personal information impact assessment	A systematic process for evaluating the potential impact of information processing risks that is likely to affect the privacy rights of individuals.
Policies	Clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organisation
Policy	Clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organisation
Private Body	A natural person or partnership who carries or has carried on any trade, business or profession but only in this capacity.
Process	A set of interrelated or interacting activities that transforms inputs into outputs
Processing	Any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as; collection, recording, organisation, collating, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Profiling	Any form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
Public Body	Any department of state, administration in the National or Provincial sphere of government or any Municipality in the local sphere of government.
Record	Means any recorded information, regardless of its medium or form, including: • Writing on any material; • 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; • Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

	• Book, map, plan, graph or drawing; • 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.
Regular and systematic monitoring	Examples include - operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g. credit scoring, fraud prevention or detection); location tracking (for example, by mobile apps); loyalty programs; behavioural advertising; fitness and health data via wearable devices; CCTV; connected devices.
Responsible Party	The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.
Restriction	To withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information - for example - temporarily moving the data to another processing system, making the data unavailable to users, or temporarily removing published data from a website.
Risk	A threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided or mitigated through pre-emptive action.
Security compromise	A security compromise means a security compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored or otherwise processed.
Special personal information	Personal information including religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, criminal, health or sex life or biometric information.
Technical and organisational measures	Internal policies as well as measures which meet the conditions of privacy, inter alia - minimising the processing of personal information; de-identifying personal information as soon as possible; transparency with regard to the functions and processing of personal information; enabling the data subject to monitor the data processing; using Operators who provide the appropriate guarantees; ensuring the appropriate security measures, including confidentiality; maintaining data quality; conducting privacy impact assessments; on-going training and awareness of staff.
The Information Officer:	Is responsible for ensuring the organisation's compliance with the POPI Act. Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties as contemplated in section 1 of the Promotion of Access to Information Act or in relation to a public body means an information officer or deputy information officer as contemplated in terms of sections 1 or 17 of the Promotion of Access to Information Act Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing

	his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
The Regulator	The Information Regulator established in terms of section 39 of POPIA

4. LEGISLATION

Records are held in accordance with the following legislation:

Basic Conditions of Employment Act 75, 1997
Businesses Act 71, 1991
Companies Act 71, 2008
Constitution of the Republic of South Africa, 1996
Consumer Protection Act 68, 2008
Electronic Communications Act 36, 2005
Electronic Communications and Transactions Act 25, 2002
Employment Equity Act 55, 1998
Financial Intelligence Centre Act 38, 2001
Hazardous Substances Act 15, 1973
Income Tax Act 58, 1962
Labour Relations Act 66, 1995
National Credit Act 34, 2005
National Environmental Management Act 107, 1998
Occupational Health and Safety Act 85, 1993
Promotion of Access to Information Act 2, 2000
Protection of Personal Information Act 4, 2013
Skills Development Act 97, 1998
South African Revenue Service Act 34, 1997
Unemployment Insurance Act 63, 2001
Unemployment Insurance Contributions Act 4, 2002
Value-Added Tax Act 89, 1991

It is possible that the above list is incomplete. If it comes to anybody's attention the list will be updated accordingly.

5. THE INFORMATION OFFICER FUNCTION

The Information Officer's main role is to encourage compliance with POPI throughout the organisation and create a culture wherein the protection of privacy is considered in all levels of decision making. The IO must ensure that all private data held by the company is protected with both physical security measures as well as best practice behaviours. The IO must be registered with the regulator before taking up any duties.

Other Responsibilities of an Information Officer:

- Deal with requests made to the organisation relative to POPI.
- Cooperate with the Regulator in relation to any inquiries.
- That this Compliance Manual is developed monitored, maintained, and made available.
- That internal measures are developed together with adequate systems to process requests for information or access to information.

- The Board of Directors are kept updated about information protection responsibilities and any case of security breaches.
- Update any policies and terms to consider POPI regulations.
- Ensure the staff's awareness of all POPI requirements.
- Remain up to date with any important changes to legislation, and
- That copies of the manual are provided to persons at their request. Hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

Documentation held by the Information Officer

- All risks, incidents, and threats
- All responses to risks, incidents, and threats
- Details of the breach, i.e., time, place, format of data, size of breach, reasons, and possible consequences, etc.
- An action plan to remedy the breach with the roles and responsibilities of all parties related to the matter.
- The Company has forms and written procedures for all steps related to the stages of breach.

The following information are recorded and managed by the POPI officer. Select which actions will be implemented by your Information Officer.

- An inventory of all data subjects and their personal information.
- Data subject consents and instructions
- The identities of the data processors
- How the data flows into and through the Company to date of destruction
- How access control is addressed
- The purpose for holding subject data

6. WHAT PERSONAL INFORMATION CAN BE COLLECTED?

According to the POPI Act, a company is deemed to be a general trader that engages in all aspects of business. The data subjects are made aware of what personal information is being collected and the reason for collecting it. The act also applies to other than a natural person; it includes companies or other legally recognised organisation. All organisations are seen as data subjects and are afforded the same right of protection.

The definition of Personal Information as stated in the POPI Act is:

*"**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:*

1. *information relating to the race, gender, sex, pregnancy, marital status, family details, nationality, 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;*
2. *information relating to the education or the medical, financial, trade union memberships, criminal or employment history of the person;*
3. *any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;*
4. *the biometric information, visual images of individuals captured on CCTV of the person;*
5. *the personal opinions, views or preferences of the person;*
6. *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;*
7. *the views or opinions of another individual about the person; and*
8. *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;"

5.1 Personal information can be processed in some of the following categories:

a. Employee's information (Human Resources and Staff Administration)
b. Clients
c. Marketing and Sales
d. Financial and Tax Records
e. Accounting Records
f. Suppliers/Vendors
g. Shareholders
h. Statutory Records (MOI, Register of Directors, etc.)
i. Websites, social media, Public Viewers, Contact Us
j. Banking institutions

The company do not collect special information about our stakeholders, personnel and clients such as religion, health, political beliefs or sexual orientation.

7. HOW IS PERSONAL INFORMATION COLLECTED?

When it comes to the storing, accessing and sharing of personal information, there is a responsibility to protect such information inside the organisation.

> POPIA applies to the processing of personal information of the "DATA SUBJECT" and according to the POPI Act, Section 3(1)(a) and Section 3(1)(b). Quote: "personal information entered in a record by or for a responsible party by making use of *automated or non-automated means*, provided that when the record of personal information is processed by ***non-automated means*** (e.g. paper and text, photographs, x-rays), it forms part of a ***filing system*** or is intended to form part of a filing system and in terms of Section 3 (1)(b)(i), the responsible party is domiciled in the Republic or in terms of Section 3(1)(b)(ii) the responsible party is not domiciled in the Republic, but makes use of automated or non-automated means, unless the processing relates only to the forwarding of personal information.

The company information is hosted by external service providers and all the information is stored on the cloud. The information may include, but are not limited to Metadata, IP addresses, contact information, names, web page access and other data generated through the websites.

The External hosts are used to fulfil a contract with our potential and existing customers and in the interest of secure, efficient and fast provision of our online services by a professional service provided. Our host will only process data to the extent necessary to fulfil its business obligations and to follow our instructions with respect to such data. Personal information will only be disclosed to third-parties, if needed in the business operations, and not for marketing and credit reporting.

THE COMPANY COLLECT PERSONAL INFORMATION THROUGH THE FOLLOWING METHODS:

1. **From the data subject self:**
    a. By contacting the company, placing an order, or creating an account
    b. Registering for events, workshops, or seminars with the company
    c. Completing online forms or replying to communication sent from the company
    d. Job Applications
    e. Emailing the company

On most platforms of engagement between the Data subjects and company, the data subjects will be informed that the company complies with the POPIA and PAIA.
Copies of any communication sent to clients with regards to the POPIA and PAIA acts will be held by the Information Officer.

8. WHERE IS PERSONAL INFORMATION ACCESSED, PROCESSED AND SHARED?

This section identifies where personal information can be accessed and used, relevant to the functions performed by the company, its employees and its clients and other third-party stakeholders.

Disclosure of personal information entails the processing of a data subject's information, only for the sole purpose for which the information was collected in order for the company to be able to do its work.

Processing can also be defined as the collection, recording, collation, storage, retrieval and alteration which could include the processing of recorded material, e.g. video or photos taken during an event.

The XSYS Global Privacy Policy guarantees that XSYS has adopted reasonable and appropriate physical, technical and administrative procedures and measures that are designed to prevent unauthorized access or disclosure, maintain data accuracy, and ensure appropriate use of the information provided. The personal information you provide is stored in secured office spaces or in computer systems located in controlled facilities, both with limited access. When we transmit highly confidential information over the internet, we protect it through the use of encryption and other safeguards. If we need to send documentation in paper, we use only trust couriers or delivery companies.

8.1 INTERNAL DOCUMENTATION

Registers and documents pertaining to transactions relevant to the data subject's personal information:

a. Annual Financial Statements
b. Management Reports
c. Customer and Vendor Agreements
d. Bank records
e. Emails
f. Agendas and Minutes of Board and Shareholder meetings and decisions
g. Audit reports
h. ID's and proof of residence of all shareholders and directors
i. Employee Agreements / registers
j. Employment Applications
k. Training manuals/ material and other manuals
l. Rental agreements
m. Invoices

8.2 HARDWARE OF COMPANY OWNED DEVICES AND USED FOR BUSINESS PURPOSES

Hardware and Software used. These include but are not limited to as at *31 May 2023*:

a. Hardware.
3 Company owned notebooks/laptops

8.3 THIRD PARTY STAKEHOLDERS – INTERNAL RELATED

3rd Party access and processing include but are not limited to:

The Company identified Local and International third-party stakeholders who may have an interest in the personal information held by the Company.

These include but are not limited to:

a. Other owned XSYS owned business entities
b. Agents or distributors of company products
c. Auditors (Internal and/or External)
d. BEE verification agency and consulting company
e. Clients of the company
f. Company Attorney
g. Company Secretarial Services Company
h. Employees in Companies
i. HR and Payroll Employees
j. Tax consultants for the Company
k. Vendors to the Company

There may occasionally be strategic or other business reasons that prompt XSYS to sell, buy, merge or otherwise reorganize businesses in some countries. Those corporate restructuring situations may involve the disclosure of personal information to prospective or actual purchasers, or the receipt of it from sellers. It is XSYS practice to seek appropriate protection for information in these types of transactions.

We may disclose information to third parties for legal or compliance purposes and responsibilities, such as to protect the security of the website or to help detect fraud. We may also use collected data for the purpose of managing any kind of dispute, including litigation.

8.4 THIRD PARTY INSTITUTIONS – EXTERNAL RELATED

3rd Party Institutions involved with the company in terms of submissions and registrations of Directors and Shareholders:

a. B-BBEE Commission
b. DOH - Department of Labour
c. SAPA – South African Payroll Association
d. SARS - South African Revenue Services

Records of personal information may be retained for periods in excess of the period for which the information was used for historical, statistical or research purposes with appropriate safeguards against the records being used for any other purposes.

9. CONSENT FROM DATA SUBJECT

The Protection of Personal Information Act 4 of 2013 (POPIA) protects information personal to individuals and businesses (Data Subjects).

The owner of information is the data subject.

All other relevant parties are deemed to be processors of personal information. POPIA requires Data Subjects to instruct processors on the obtaining, use, purpose of use and destruction of personal information.

The data subject remains the owner of his or its personal information.

The classification of collection of information directly from a data subject or other as stated in the POPI Act is:

12. (1) Personal information *must be collected directly from the data subject, except as otherwise provided for in subsection (2)*

(2) It is not necessary to comply with subsection (1) if -

- *a) information is contained in or derived from a public record or has deliberately been made public by the data subject;*
- *b) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;*
- *c) collection of the information from another source would not prejudice a legitimate interest of the data subject;*
- *d) collection of the information from another source is necessary –*
  - *i. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;*
  - *ii. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);*
  - *iii. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;*
  - *iv. in the interests of national security;*
  - *v. to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;*
- *e) compliance would prejudice a lawful purpose of the collection; or*
- *f) compliance is not reasonably practicable in the circumstances of the particular case.*

10. RIGHTS OF THE DATA SUBJECT

A data subject has the right to have his/her personal information processed in accordance with the conditions of the law as set out below.

1) **The right to access personal information**
   The data subject has the right to know what personal data is held by the company and can request to access that data.

2) **The right to have personal data corrected or removed.**
   The data subject may request that information held be corrected, updated or removed.

3) **The right to object to processing of personal information.**
   On reasonable grounds, the data subject can object to the processing of their information.

4) **The right to complain to the Information Regulator.**
   If the data subject feels that there is an infringement in connection with POPIA, a complaint can be lodged with the Information Regulator in respect of a determination by an adjudicator.

5) **The right to be informed**
   Collection of personal information must be communicated to the data subject, especially regarding unlawful access.

Should the client's consent be required to process their personal information the client has the right to withdraw their consent.

11. DATA SECURITY SAFEGUARDS AND STORAGE

The POPI Act states that the responsible party (company) must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent unlawful access and processing of personal information.

POPIA applies to both hard copies and electronic (soft) copies of personal information. The company must ensure that their existing IT infrastructure complies with POPIA requirements regarding the protection of personal information. The assistance of the IT administrator/consultant will be required in connection with the security aspects of the IT infrastructure. Information can be kept physically in hard copies or electronically format.

XSYS's Internet pages use cookies, local storage and session storage. This is to make our offer more user-friendly, effective and secure. Local storage and session storage is a technology used by your browser to store data on your computer or mobile device. Cookies are text files that are stored in a computer system via an Internet browser. You can prevent the use of cookies, local storage and session storage by setting them in your browser.

Cookies allow XSYS to recognize website users. The purpose of this recognition is to make it easier for users to utilize our website. The website user that uses cookies, e.g. does not have to enter access data each time the website is accessed, because this is taken over by the website, and the cookie is thus stored on the user's computer system.

11.1 SECURITY SAFEGUARDS WITHIN THE ORGANISATION

Electronic Security features are utilized by the External hosts to mitigate the risks associated with the Act and the company has the following security safeguards in place:

Nr	Description
1.	All company officials, employees, vendors and clients are appropriately informed of measures taken to protect personal information and the processing of personal information.
2.	Only authorised persons have access to the minimum personal information as required for the purpose.
3.	All workstations are password-protected, with restricted access and passwords are changed at regular intervals.
4.	Digital profiles and permissions of staff that left the company are terminated and all access to personal information is blocked.
5.	Those who hold or process information consent to full surveillance of processing of personal information and consent to personal accountability for such processing.
6.	All data processors committed to protect personal information and to procure instruction on deemed processing. Confidentiality agreements are signed by all data processors.
7.	The Company obtained the commitment of all processors of personal information to ensure maximum security and secrecy on all personal information and to personally assume the responsibility to employ measures to protect personal information on all electronic equipment.
8.	It is important that company's devices are always kept on the processor's person. Neither the device nor any information on the device is ever given to any third parties who do not hold the written consent of the data subject.
9.	Least number of security access codes are kept by least number of employees. The data specialist appointed by the Company will take into account all risk factors and address same to the satisfaction of the POPI Act.
10.	Business data will always be kept separate from personal data – i.e., personal information.

11.2 ELECTRONIC SECURITY SAFEGUARDS WITHIN THE ORGANISATION

Nr.	Description
1.	All individual or network connected devices are protected by a Firewall.
2.	All individual or network connected devices anti-malware.
3.	All individual or network connected devices are protected by anti-virus software.
4.	Upon exiting, former employees are removed as users on all electronic systems and devices.

11.3 HARD COPY (NON-ELECTRONIC) SAFEGUARDS WITHIN THE ORGANISATION

Hard copies of company statutory documents will be stored according to the relevant legislation and company policies. The following apply:

a. Personal information is kept safe, and rules and regulations are applicable to access filing facilities and office spaces.

12. SECURITY BREACHES AND INCIDENT MANAGEMENT

In an event where personal information of a data subject is compromised and accessed unlawfully it is the responsible party's (the company's) responsibility to notify the Information Regulator as well as the affected parties as soon as reasonably possible. The act does however take into account delayed notifications of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determined that notification would impede on a criminal investigation by the public body concerned.

The company has approved procedures to manage incidents that may have an impact on POPIA and PAIA.

12.1 INCIDENT MANAGEMENT POLICY

The company has an **Incident Management Policy** in place which includes the following:

Nr	Description
1.	The Company identified procedures to manage incidents that may have an impact on the POPI Act.
2.	Roles and responsibilities are known to all responsible data processors and ready to be implemented when incidents occur.
3.	All heads of departments are in full control of all personal data and vowed to keep personal data safe and secure.
4.	Steps have been taken to reduce incidents and to increase the speed in which incidents are attended to.
5.	Processors of personal information are forewarned to report incidents as soon as possible and managers are forewarned to attend to reports as soon as possible as set out in the DPA.
6.	Operators will inform the responsible party (company) immediately when a security breach is detected.
7.	Subject to exceptions in section 22 which covers investigations, the responsible party and the Regulator will be notified immediately of compromised security.

12.2 SECURITY BREACHES

Data breach action plans can include but are not limited to, the following:

1. All parties related to the incident will assist one another to attend to a breach as soon as possible with maximum allowed force.
2. When an incident occurs, the incident, in compliance with the POPI Act will not be discussed with anyone but the employee's direct manager.
3. Managers may only discuss incidents with the Information Officer.
4. The Information Officer may only discuss the matter with the board of directors, where after the board will direct the CEO.
5. Once a breach is confirmed, the Information Officer will communicate, as prescribed by the POPI Act, with the affected data subject, the Regulator and those who may be influenced by the breach.
6. The following will be documented:
    a. All risks, incidents, and threats.
    b. All responses to the above.
    c. Details of the breach, i.e., time, place, format of data, size of breach, reasons and possible consequences, etc.
    d. An action plan to remedy the breach with the roles and responsibilities of all parties related to the matter.
    e. The Company has forms and written procedures for all steps related to the stages of breach.

If you have comments or questions about our privacy statement, or any concerns or a complaint regarding our collection and use of your personal data or a possible breach of your privacy, please email us at **data.protection@xsysglobal.com** or alternatively contact our Information Officer.

12.3 INFORMATION OFFICER MAINTAINED RECORDS

The Information officer can keep the following details:

Nr	Description
1.	All risks, incidents, and threats.
2.	All responses to risks, incidents, and threats.
3.	Details of the breach, i.e. time, place, format of data, size of breach, reasons and possible consequences, etc.
4.	An action plan to remedy the breach with the roles and responsibilities of all parties related to the matter.
5.	The Company has forms and written procedures for all steps related to the stages of breach.

The following information can be recorded and managed by the Information officer:

Nr	Description
1.	The identities of the data processors.
2.	How access control is addressed.
3.	The purpose for holding subject data.

A copy of the following related policies is kept by the Information Officer:

Policy name	Last updated
XSYS Global Personal Data Breach Procedure	26/01/2023
XSYS Global Personal Data Privacy Policy	26/01/2023

13. THE REGULATOR'S GUIDE

The Regulator's Guide has been compiled and published by the INFORMATION REGULATOR to assist persons in using and understanding PAIA, as provided for in Section 14 of PAIA.

The purpose of the **Regulator Guide** is to assist people in making requests for information under PAIA, a list of types of information that can be requested using PAIA and a step-by-step guide on how to use PAIA to make a request for information.

13.1 The **Regulator Guide** is available in each of the official languages and in braille.

13.2 The **Regulator Guide** contains the description of-

13.2.1 the objects of PAIA;

13.2.2 the postal and street address, phone and fax number and, if available, electronic mail address of-

13.2.2.1 the Information Officer of every public body, and

13.2.2.2 every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA[1];

13.2.3 the manner and form of a request for-

13.2.3.1 access to a record of a public body contemplated in section 11[2]; and

13.2.3.2 access to a record of a private body contemplated in section 50[3];

13.2.4 the assistance available from the IO of a public body in terms of PAIA;

13.2.5 the assistance available from the Regulator in terms of PAIA;

13.2.6 all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA, including the manner of lodging-

13.2.6.1 an internal appeal;

13.2.6.2 a complaint to the Regulator; and

13.2.6.3 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;

---

[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 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.*

[3] *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.

13.2.7 the provisions of sections 144 and 515 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

13.2.8 the provisions of sections 156 and 527 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

13.2.9 the notices issued in terms of sections 228 and 549 regarding fees to be paid in relation to requests for access; and

13.2.10 the regulations made in terms of section 92[10].

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

13.4 The **Regulator Guide** can also be obtained-

13.4.1 upon request to the Information Officer;

13.4.2 from the website of the Regulator https://www. https://inforegulator.org.za/paia-guidelines/.

A copy of the PAIA Guide is available for inspection at the offices of the Information Regulator.

Contact details are as follows:

Address:	27 Stiemens Street, Braamfontein, Gauteng, South Africa
Post:	Information Regulator (South Africa), PO Box 31533, Braamfontein, 2017
Telephone:	010 023 5287
Website:	inforegulator.org.za
E-mail:	enquiries@inforegulator.org.za

[4] *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.*

[5] *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.*

[6] *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*

[7] *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*

[8] *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.*

[9] *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.*

[10] *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."

14. PROCEDURE FOR REQUESTING ACCESS TO INFORMATION

It is important to note that the successful completion and submission of an access request form does not automatically allow the requester access to the requested record. An application to access to a record is subject to certain limitations if the requested record falls within a certain category as specified with Part 3 and Chapter 4 of the Act.

Completion of Access Request Form

In order to facilitate a timely response to requests for access, all requesters should be aware of the following when completing the Access Request Form:

a. The Access Request Form must be completed (refer Annexure A).
b. Proof of identity is required to authenticate the identity of the requester. Therefore, in addition to the access form, requestors will be required to supply a copy of their identification document.

i. Complete the form in BLOCK LETTERS and answer every question.
ii. If a question does not apply state N/A in response to that question
iii. If there is nothing to disclose in reply to a particular question state "nil" in response to that question.
iv. If there is insufficient space on a printed form, additional information may be provided on an attached folio
v. When the use of an attached folio is required, precede each answer with the applicable title.

Submission of the Access Request Form

The complete Access Request Form together with a copy of the identity document must be submitted either via post or e-mail and must be addressed to the contact person as indicated above.

This fee is not applicable to personal requesters referring to any person seeking to access records that contain their personal information.

An initial, request fee of R40.00 (including VAT) is payable on submission. Refer to Annexure A under Fees for breakdown of fees.

Payment of Fees

Payment details can be obtained from the contact person as indicated above. If the request for access is successful an access fee may be required for the search, reproduction and/or preparation of the record(s) and will be calculated based on the Prescribed Fees.

Proof of payment must be supplied, and the access fee must be paid prior to access being given to the requested record.

If a deposit has been paid in respect of a request for access which is refused, then the information officer must refund the deposit to the requestor

Notification

The company has leeway of 30 days from receipt of the request to decide whether to grant or decline the request and give notice with reasons to that effect.

The 30-day period within which the company has to decide whether to grant or refuse the request, may be extended for a further period of not more than thirty days, if the request is for a large volume of information and the information cannot be reasonably obtained within the original 30-day period. The company will notify the requester in writing should an extension be needed.

Complaints to the Information Regulator

A requester may approach the Information Regulator to lodge a complaint in accordance with Section 77(a) of PAIA on a prescribed form and the form can be sent by email to: PAIAComplaints@inforegulator.org.za

A requester or third party may only submit a complaint to the Regulator after that requester or third party has exhausted the internal appeal procedure against a decision of the Information Officer of a public body or head of private body.

15. REFUSAL OF ACCESS TO RECORDS

The main grounds for refusal of a request for information are set out below:

- Mandatory protection of the privacy of a third party who is natural person, which would involve the unreasonable disclosure of personal information of that natural person.
- Mandatory protection of the commercial information of a third party, if the record contains:
    - Trade secrets of that party
    - Financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of that party
    - Information disclosed in confidence by a third party to the company if the disclosure could put that third party to a disadvantage in negotiations or commercial competition
- Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.
- Mandatory protection of the safety of individuals and the protection of property.
- Mandatory protection of records which could be regarded as privileged in legal proceedings.

16. RECORDS AVAILABLE WITHOUT REQUEST

In terms of the Act, Section 51(1)(d) any records of a public nature, like those disclosed on the company's website, marketing and promotional material, brochures and in its various annual reports, may be accessed without the need to submit a formal application.

Other non-confidential records, such as statutory records maintained at CIPC, may also be accessed without the need to submit a formal application.

Other documentation that is available without a request includes this manual and the POPI Manual.

17. RECORDS ONLY AVAILABLE UPON REQUEST

In terms of the PAIA Act, Section 51(1)(d) the following records held by the Company can only be accessed upon the submission of a formal application.

This clause serves as a reference but is not limited to the categories of information that the Company may hold.

17.1 Personnel Records

17.1.1 Personal records provided by personnel.

17.1.2 Records provided by a third party relating to personnel.

17.1.3 Conditions of employment and other personnel-related contractual and quasi-legal records.

17.1.4 Internal evaluation records and other internal records.

17.1.5 Correspondence relating to personnel.

17.1.6 Training schedules and material.

17.1.7 Any person who works for or provides services to or on behalf of the company and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the company.

17.1.8 This includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff, as well as contract workers.

17.2 Customer Related Records

17.2.1 Records provided by a customer to a third party acting for or on behalf of the company.

17.2.2 Records provided by a third party.

17.2.3 Records generated by or within the company relating to its customers, including transactional records.

17.3 Private Body Records

17.3.1 Financial records, e.g.

a) Accounting Records
b) Auditor Reports
c) Debtors Records
d) Creditors Records

17.3.2 Operational records, e.g.

a) Agreements
b) Emails
c) Asset registers

17.3.3 Databases

17.3.4 Information Technology

17.3.5 Marketing records

17.4 Internal Correspondence

17.4.1 Product records

17.4.2 Statutory records, e.g.

a) Board Reports and Minutes and Resolutions
b) Memorandum of Incorporation and other forms lodged with CIPC
c) Company register
d) Shareholders register

17.4.3 Internal Policies and Procedures

17.4.4 Records held by officials of the institution - these records include, but are not limited to, the records which pertain to the company's own affairs.

17.5 Other Party Records

17.5.1 Personnel, customer or private body records which are held by another party, as opposed to the records held by the company itself.

17.5.2 Records held by the company pertaining to other parties, including without limitation, financial records, correspondence, contractual records, records provided by the other party, and records third parties have provided about the contractors/suppliers.

17.5.3 The company may possess records pertaining to other parties, including without limitation contractors, suppliers, subsidiary/holding/sister companies, joint venture companies, and service providers. Alternatively, such other parties may possess records that can be said to belong to the company.

As per the Act, the destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

PS: Note that the accessibility of the records may be subject to the grounds of refusal set out in this PAIA Manual and in line with the PAIA Act.

ANNEXURE A: ACCESS REQUEST FORM

(Section 53(1) of the Promotion of Access of Information Act, 2000 (Act No 2 of 2000) [Regulation 10]

Particulars of Private Body

Requests can be submitted either via post or e-mail and should be addressed to the relevant contact person as indicated below:

Contact person	GORDON SMITH
Postal Address	91 MIMETES ROAD, DENVER EXT 4, JOHANNESBURG, GAUTENG, 2094
Physical Address	91 MIMETES ROAD, DENVER EXT 4, JOHANNESBURG, GAUTENG, 2094
Phone number	082 443 7319
E-mail	gordon.smith@xsysglobal.com

Particulars of person requesting access to the record

(a) The particulars of the person who requests access to the record must be given below

(b) The address and/or fax number in the Republic to which the information is to be sent must be given

(c) Proof of capacity in which request is made, if applicable, must be attached

Full names and surname	
Identity Number	
Physical Address	
Postal Address	
Telephone number	
E-mail address	

Capacity in which request is made, when made on behalf of another person	

Particulars of person requesting access to the record (if a legal entity)

(a) The particulars of the entity who requests access to the record must be given below

(b) The address and/or fax number in the Republic to which the information is to be sent must be given

(c) Proof of capacity in which request is made, if applicable, must be attached

Name of entity	
Registration number	
Physical Address	
Postal Address	
Telephone number	
E-mail address	

Particulars of person on whose behalf request is made

This section must ONLY be completed if a request for information is made on behalf of another person

Full names and surname	
Identity Number	

Particulars of record

(a) Provide full particulars of the record to which access is requested, including the reference number if it is known to you, to enable the record to be requested

(b) If the provide space is inadequate, please use a separate folio and attach it to this form. Please sign additional folios

Description of record of relevant part of the record

Reference number (if available):	
Any further particulars of record:	

FEES

(a) A request for access to a record, other than a record containing personal information about yourself will be processed only after a request fee has been paid.

(b) 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.

(c) If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption of payment of fees:

FORM OF ACCESS TO RECORD

Form in which record is required - Mark the appropriate box with an **X**

NOTES

(a) Compliance with your request in the specified form may depend on the form in which the record is available

(b) Access in the form requested may be refused under certain circumstances. In such a case you will be informed whether access will be granted in another form

(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:
   Copy of record ☐ Inspection of record ☐

2. If record consists of visual images:
   View the images ☐ Copy of the images ☐ Transcription of the images ☐

3. If the record consists of recorded information that can be reproduced in sound:
   Listen to the soundtrack (audio) ☐ Transcription of soundtrack ☐

4. If the record is held on computer or in an electronic or machine-readable form
   (this includes photographs, slides, video recordings, computer generated images, sketches etc.)
   Printed copy of record ☐ Printed copy of information derived from the record ☐ Copy in computer readable form ☐

If you requested a copy or transcription of a record (above) do you wish the copy of transcription to be posted to you? Postage is payable

Yes ☐ No ☐

In the event of a disability

If you are prevented by a disability from reading, viewing or listening to the record in the form of access provided for in 1 to 4 above, state your disability and indicate in the form in which the record is required

Disability:	**Form in which record is required:**

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED

If the space provided is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all folios

1. Indicate the right to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

NOTICE OF DECISION REGARDING REQUEST FOR ACCESS

You will be notified in writing whether your request has been approved or denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

_____

_____

Signed at ……on this ..... day of..... 20 .....

SIGNATURE OF REQUESTER/ PERSON ON WHOSE BEHALF REQUEST IS MADE

	YOU MUST
1.	Complete all necessary spaces
2.	Sign the access request form
3.	Sign additional folios completed

	SEND WITH THIS APPLICATION
1.	The request fee (if not personal requester)
2.	Any additional folios completed
3.	Copy of Identity Document

FEES

Prescribed Fees in terms of the (Section 54(7) of the Promotion of Access to Information Act, 2000 (Act No.2 of 2000) [Fees for record of Private Body]

PLEASE NOTE THAT ALL PRICES LISTED BELOW ARE INCLUSIVE OF VALUE ADDED TAX

(a)		For every photocopy of an A4 size page or part thereof	R	1.10
(b)		For every printed copy of an A4 size page or part thereof held on computer or in an electronic or machine-readable form	R	0.75
(d)	(i)	For a transcription of visual images, for an A4 size page or part thereof	R	40.00
	(i)	For a copy of visual images	R	60.00
(e)	(i)	For a transcription of an audio record, for an A4 size page or part thereof	R	20.00
	(ii)	For a copy of audio record	R	30.00
(f)		To search for and prepare the record for disclosure – R50.00 for each hour or part thereof reasonably required for such search and preparation		

(Section 54(2) of the Promotion of Access to Information Act, 2000 (Act No.2 of 2000) [Regulation 11(3)]

PLEASE NOTE THAT ALL PRICES LISTED ABOVE ARE INCLUSIVE OF VALUE ADDED TAX

(a) Six hours as the hours to be exceeded before a deposit is payable; and
(b) One third of the access fee is payable as a deposit by the requester;
(c) The actual postage fee is payable when a copy of a record must be posted to a requester