Information Security Management System Requirements for GDPR and POPI act

All requirements to ensure that this procedure will provide consistent customer satisfaction and ensure security of confidential information have been defined and documented in this procedure and in the documented Information Security Management System procedures:

- Document and Control of Records Process
- Control of Non-Conforming Services Process
- Corrective and Preventive action Process
- Internal Audit & Management Review Process
- Statement of Applicability
- Risk Management Process

Table of Contents

Uncontrolled copy when printed

1 Introduction

The relationship of Saryx Engineering Group with its clients, employees and directors is based on mutual integrity and trust and it is always therefore committed to maintaining this trust by protecting the privacy of personal information and data disclosed and received from any data subject or data owner and to the best of its ability.

The Management of Saryx Engineering Group subscribes to the goals and principles of data privacy and information security in line with relevant legislation and its business strategy and objectives. Data privacy and information security is an integral component of the information management structure of Saryx Engineering Group.

Saryx Engineering Group has an obligation to ensure appropriate security of all Information Technology (IT) systems (data, equipment and processes) and personal information that it owns and/or controls on behalf of other responsible parties.

The need for data privacy and information security is driven by:

- Legal, statutory, regulatory and contractual obligations;
- Risk assessment
- Operational objectives and requirements for information systems that Saryx Engineering Group has developed.

Saryx have a well-documented Information Security Management policy which contains the IT security elements and responsibilities ISMP.01- Information Security Management Policy (ISMP)

2 Definitions

1. **Data subject**: The person to whom personal information relates;

2. **POPIA**: Refers to the Protection of Personal Information Act 4 of 2013;

3. **GDPR:** Refers to the General Data Protection Regulation (EU) 2016/679

4. **Processing**: 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 merging, linking, as well as restriction, degradation, erasure or destruction of information.

5. **Records**: any recorded information regardless of form or medium, including any of the following;

   (a) writing of material;

   (b) information produced, recorded or stored digitally or Physically or any material subsequently derived from information so produced, recorded or stored;

6. **Responsible party:** means a public or private body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information.

7. **Personal Information** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

3 Objectives

- POPIA and GDPR requires consumer to be aware as to the manner in which their personal information is used, protected, disclosed and destroyed.
- Saryx Engineering Group guarantees its commitment to protecting the consumer's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.
- This Policy sets out the manner in which Saryx Engineering Group deals with the consumer's personal information and stipulating the purpose for which said information is used.

The **purpose** of this policy is to enable Saryx Engineering Group to comply with;

a) Protection of Personal Information Act, 2013 (hereinafter POPIA Act)
b) General Data Protection Regulation (hereinafter GDPR)
c) Adhere to both Legislative requirements.

Since there is overlap between the POPIA act and GDPR which ever requirement of either of the Two acts is most restrictive will be applied. For example the minimum age of data subject consent is 16 years of age in the EU whereas in South Africa the Legal age is 18. In this instance the most restrictive would be South Africa.

4 Compliance to Protection of Personal Information and GDPR.

4.1 Data subjects pertaining to Saryx have the following rights;

- Objection to the use of personal information.
- Notification if information is being used for something other than what was consented for.
- Establishing whether the responsible party holds information.
- Request that information can be corrected, destructed or deleted.
- Refuse processing for direct marketing by unsolicited electronic communications.
- Lodge a complaint with the Information Regulator.
- Institute civil proceedings.(Sec 99)
- correct or delete Personal Information that is inaccurate, irrelevant, excessive, incomplete, misleading or obtained unlawfully; .

4.2 Conditions for lawful processing

4.2.1 Accountability

- The Responsible party must ensure that the conditions set out in the POPIA Act and GDPR and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

4.2.2 Processing Limitations

- The Data subjects must consent.
- Consent is necessary to carry out actions to conclude or perform a contract to which the data subject is a party.
- Processing compliance with an obligation imposed by law.
- Must process to protect the legitimate interest of data subject.
- Pursue legitimate interest of other responsible party or third party to whom the information was supplied.
- The Data subject may withdraw consent.
- The Data subject may object on reasonable grounds.
- The Data subject must be at least 18 years of age.

4.2.3 Specific Purpose

Personal Information must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the responsible party. The data subject must be made aware of the purpose of the collection.

Records must not be retained any longer than is necessary for achieving the purpose for which it was collected unless;

- further retention is required by law;
- the responsible party is reasonably required to keep it;
- retention is required by a contract between the parties;

4.2.4 Limitations of Retention of personal information

- The data subject consents to the further retention.
- Personal Information must be destroyed, deleted or de-identified as soon as is reasonably practical.
- Destruction or deletion must be done in a manner that prevents its reconstruction in an intelligible form.
- The information officer shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval, unless the new purpose is required by law.;
- The information officer shall ensure that a person collecting personal information will be able to explain to the individual why this is being done;
- The Information officer shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why personal information is to be collected.

Limiting collection and further processing

Will be in accordance or compatible with the purpose for which it was collected by Saryx. The Responsible Party shall ensure that personal information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to fulfil the specific purpose for which the Personal Information is being collected.

Personal Information may only be processed if:

- The data subject consents to the processing;
- processing is necessary for the conclusion or performance of a contract to which the data subject is a party;
- there is a legal obligation to do the processing;
- processing protects the legitimate interests of the data subject; • processing is necessary for the proper performance of a public law duty by a public body;
- processing is necessary for the pursuit of legitimate interests of the responsible party.
- A data subject may object, at any time, on reasonable grounds, to the processing of their Personal Information. The re sponsible party may then no longer process the Personal Information.

Personal Information must be collected directly from the data subject except if:

- the information is contained in a public record or has deliberately been made public by the data subject;
- the data subject has consented to the collection from another source;
- Collection from another source would not prejudice a legitimate interest of the data subject;

4.2.5 Security Safeguards

To manage POPIA and GDPR compliance effectively, Saryx Engineering Group had included the compliance in to the existing IS027001 Risk Management process.

The company uses a data centre service provider, Xneelo who have a detailed page which defines the hosting options available and legalities around each one. https://xneelo.co.za/legal/specific-terms-and-conditions/hosting-terms/. There is a formal SLA regarding the hosting agreement in place with Xneelo and actions that need to be taken should the contract end between the 2 parties.

Xneelo security document, https://xneelo.co.za/legal/security

5 Data storage

Saryx Engineering Group keeps track of Data Storage locations (Servers and Physical Location) as well as Data Classification.

5.1 Offshoring of Data

Both the POPIA act and GDPR pose limitation on the Offshoring of personal information.

GDPR: Personal information may not leave the South African boarder, unless the Data Processor complies with GDPR.

POPIA: Personal information may not leave the South African boarder, unless the Data Processor complies with the POPIA act.

6 Responsibilities:

Information Security Officer:
Saryx have formally appointed a Data Protection Officer who has the following key responsibilities and authority to manage,

- Ensure compliance with POPIA and GDPR,
- Develop and maintain the Security Policies
- Periodic awareness communications take place
- Ensuring that Internal and External Privacy Notices are published.
- Handling data subject access requests
- Assess the privacy requirements and responsibilities of information processing service providers or operators in terms of sections 20 and 21 of POPIA.
- Function as the GDPR Data Protection Officer (DPO)

7 Processes Procedures

7.1 Do not contact (DNC) process

When a customer notifies Saryx Engineering Group, either directly to the Customer Service Representative or via any one of the public communication channels the request is to be sent one of the executive team who will log a ticket on HSEC Online Service Desk and the team will add the person to the DNC database.

7.2 Data Deletion Process

7.2.1 Call Centre Process

When a customer notifies Saryx Engineering Group, either directly to the Customer Service Representative or via any one of the public communication channels the request is to be sent one of the executive team will log a ticket on HSEC Online Service Desk and the team will add the person to the DNC database.

7.2.2 Recruitment and Offboarding Process

The recruitment team provides a link through their recruitment platform for unsuccessful candidates to have their information removed from the platform. Information from candidates are stored in case a suitable position becomes available. Also addressed in the ISO27001 ISMS.

When staff join Saryx they sign confidentiality and NDAs which is a mandatory document for employees on HSEC Online.

All user login IDs are audited at least twice yearly, and all inactive logon IDs are revoked. Each individuals logon access is directly linked to the status of their employee on HSEC Online, on termination the HSEC Online access is automatically revoked. The Company Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts. The account will be locked for 10 minutes, and then the user can try to log on again.

Users who desire to obtain access to Company systems or networks must have a completed and signed Network Access Form. This form must be signed by the supervisor or department head of each user requesting access.

7.3 Suppliers and Providers

7.3.1 Data suppliers

Any supplier process data on behalf of Saryx Engineering Group, these suppliers need to evidence their compliance to the POPIA act or GDPR during the on Boarding Phase and must be verified annually.

The company user a reputable data centre service provider who has particularly good controls in place with regards to data management, cloud services and data management. HSEC Online is hosted by in a Xneelo data centre. Xneelo provide a publicly available Legal Centre which defines their commitment and responsibilities with regards to security within the environment, https://xneelo.co.za/legal.

8 Supporting Policies

Saryx Engineering Group have a documented set of policies and procedures that have been entrenched and manged via the HSEC Online software with all data cloud based.

Saryx have a page defining Terms and conditions for users
https://www.hsec.co.za/Account/ShowTermsConditions

Xneelo have a page defining security and access control
https://xneelo.co.za/legal/specific-terms-and-conditions/

Defined in the Xneelo privacy policy
https://xneelo.co.za/legal/privacy-policy/