SCRIPT TECHNOLOGIES

DATA PRIVACY AND PROTECTION POLICY

POL ISM 003

Abstract

This Data Privacy and Protection Policy outlines the organization's commitment to safeguarding personal and sensitive information in compliance with applicable data protection laws and industry best practices. It establishes the principles, responsibilities, and procedures for collecting, processing, storing, and sharing data while ensuring transparency, security, and accountability.

DATA PRIVACY AND PROTECTION POLICY

Preface and document control

This document is intended to provide information in respect of SCRIPT policy, procedure, standards or guidance and will be periodically updated to reflect any changes due to business requirements or infrastructure. Neither all nor part of this document shall be reproduced or released for commercial purposes by a recipient without the express consent of the stated SCRIPT document owner. This document MUST be reviewed and approved by the designated SCRIPT approver(s) to ensure technical accuracy and business validity.

Document owner and approver(s)	
Owner	Script Technologies
Approver(s)	Managing Director

Version control		
Version	Version date	Document history
1	24 March 2025	Initial
2		
3		

Internal distribution list	
To all SCRIPT Employees and Subsidiaries	

External distribution

The document owner must approve any request for a copy of this document to be released to an external party. Consideration must be given to the content and classification of this document before authorisation is granted. The owner of this document must state the distribution format(s), copying permissions and procedures for document return or disposal.

TABLE OF CONTENTS

1. INTRODUCTION

This policy governs processing of your information by Script Technologies Proprietary Limited, Registration Number: 2019/291082/07 ("the Company"). By using the Company's services or interacting with the Company in person, by electronic communication or through the Company's website you agree to the terms and conditions of this privacy policy and the Company's Information Manual, which can be accessed on the link provided below.

The Company is dedicated to protecting your right to privacy and will take all reasonable steps to protect your information and to ensure that any processing of information is lawful and fully compliant with the provisions of the Protection of the Personal Information Act 4 of 2013 ("POPI"). Any reference in this Data Privacy and Protection Policy to "information" means "personal information" and "special personal information" as defined in POPI.

2. PURPOSE

The purpose of the POPI act is to give effect to the constitutional right to privacy, by safeguarding your information when processed by the Company. On the other hand, the Promotion of Access to Information Act 2 of 2000 ("PAIA") was passed to give effect to the constitutional right of access to any information held by a public or private body which is required for the exercise or protection of any rights.

PAIA and POPI aims to balance the right to privacy against other rights, particularly the right of access to information and to set the minimum standard to be followed for the processing of information to be lawful.

3. KEY DEFINITIONS AND ABBREVIATIONS

ABBREVIATION	DEFINITION
ICT	Information Communication Technology
PAIA	The Promotion of Access to Information Act No. 2 of 2000
PoPIA	The Protection of Personal Information Act No. 4 of 2013 (in this Guideline the abbreviation is used interchangeably with the "Act")

ACRONYM OR WORD	DEFINITION
Biometrics	A technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	The person to whom personal information relates. Data subjects within employment context includes applicants and former job applicants (successful or unsuccessful), former or current employees, temporary employment services staff, casual staff, staff on secondment and those on work experience placements. The personal information of all of these persons must be dealt with in accordance with POPI.
Information Officer	The Information Officer is responsible for ensuring the Company's compliance with PoPIA.
Personal Information	Information relating to an identifiable, living, natural person, and where 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 numbers, symbol, email 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 preference 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 another personal information relating to the person or if the disclosure of the name itself would reveal information about the person
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 c. Merging, linking, as well as restriction, degradation, erasure or destruction of information
Record	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 embodies 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

4. POLICY

4.1 POLICY APPLICATION

This policy and its guiding principles applies to:

- The Company's governing body;
- All divisions of the Company;
- The permanent or temporary employees and independent contractors of the Company;
- All contractors, suppliers and other persons acting on behalf of the Company;
- Any joint ventures, and/or other business organisations that are owned or controlled by the Company who receive or process personal information for, or on behalf of the Company;

- Personal information of external data subjects and data owners processed and/or stored by the Company, as well as the personal information of Company personnel.

The policy's guiding principles find application in all situations and must be read in conjunction with PoPIA as well as the Company's PAIA Manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).

PoPIA does not apply in situations where the processing of personal information:

- Is concluded in the course of purely personal or household activities, or
- Where the personal information has been de-identified.

4.2 SCOPE

The contents of this policy is applicable to all employees of the Company and has been introduced in order to encourage the protection and confidentiality of all personal information that has been made available to the Company by employees or any client or supplier or any party who has disclosed any information of a private or business nature, for the sole intention of employment, business transactions, contracts or communication and will be deemed to be necessary for the records pertaining to the Company.

The information officer is the custodian of this policy, and responsible to ensure that this policy is incorporated and implemented in the various divisions of the Company, and that training is provided to all parties concerned regarding the contents of the Protection of Personal Information Act (PoPIA).

The Company will make employees aware of this policy by discussing it during induction sessions, monthly awareness training and by distributing it to the workforce by making it available on the Company's Document Management System.

However, it remains the duty and responsibility of all employees to make themselves aware of, and to familiarize themselves with, the content and application of this document.

4.3 PURPOSE OF PROCESSING INFORMATION

The Company may lawfully process your information:

- with your consent; or
- in terms of an obligation imposed by law; or
- in terms of a written contract between you and the Company; or
- for the purpose of pursuing a legitimate interest for you or the Company.

When utilising the Company's services or interacting with the Company in person, by electronic communication or through the Company's website, the Company may process your information for the following purposes:

- to comply with legislation;
- for retention of records as required by any law, e.g. fraud and crime detection and prevention;

- for retention of records required in terms of an agreement with a third party, i.e. service level agreement;
- to render any services to the customers of the Company;
- To conduct due diligence checks on employees, customers and service providers, e.g. credit checks, SAPS Clearance information and check references;
- to obtain professional advice, e.g. from legal counsel or auditors / accountants;
- to facilitate the collection of fees for the services provided by the Company;
- the storage of the information with external storage and record management companies;
- marketing of products and services;
- track visitor activity on the Company's website;
- the storage of information in a secure cloud-based storage facility;
- to verify the accuracy, correctness, completeness of any information provided to the Company; and
- any matter ancillary thereto.

The Company will process your information to enable it to render services, to comply with its contractual obligations and to comply with any obligations imposed on the Company by law. Should the Company not receive the information, it may not be able to render services and may result in the Company being unable to comply with its legal and contractual obligations.

The types of information the Company may process and a non-exhaustive list of legislation in terms of which the Company processes such information, is detailed in the Information Manual.

The Company will only keep your information for as long as it is required to, to achieve the purpose for which it was collected or as required by law, whereafter the information will be destroyed in a manner which will render the information unintelligible and incapable of reconstruction.

Where the Company processes your information or where you have consented to the processing your information by the Company, you have the right to submit a request to the Company to withdraw your consent or to object to the processing of your information on reasonable grounds. Such request must be submitted on prescribed Form 1, which is available on request from the Information Officer.

4.4 STORAGE OF YOUR INFORMATION

The Company has implemented a comprehensive data storage and security policy aimed at protecting your information. The Company has taken reasonable technical and organisational measures to prevent the loss, damage, unauthorised destruction and unlawful access of your information.

While the Company has taken such steps to protect your information, there is no method of data security and storage which is completely protected against data breaches. Should any data breach occur which involves your information, the Company will advise you, the Information Regulator and relevant law enforcement agencies. The Company will provide you with the necessary support, information and advice relating to the data breach to allow you to mitigate the possible consequences of such breach.

4.5 SHARING OF YOUR INFORMATION WITH THIRD PARTIES

The Company may, subject to authorisation in terms of any applicable legislation, contract or with your consent, share your information with a third party in order for the Company to render the services which you require and / or to comply with any obligation placed on the Company in terms of any law or in terms of a contract.

1. The information will be shared in compliance with the Company's legal obligation to protect the integrity and confidentiality of your information and only to the extent absolutely necessary to achieve the purposes detailed in this Privacy Policy and our Information Manual.
2. The sharing of your information will be subject to the obligation of confidentiality by virtue of the position held by the person with whom the information is shared or where such person's position does not impose such an obligation of confidentiality, the Company will secure a declaration of secrecy with such person to impose the confidentiality obligations necessary to protect your information.

4.6 PLANNED TRANS-BORDER FLOW OF INFORMATION

The Company may process and store your information in a manner which may result in the trans-border flow of such information outside of the Republic of South Africa, for the purposes of, including but not limited to, cloud-based storage. The Company will ensure that the processing of your information outside of the Republic of South Africa will be subject to strict contractual obligations for the processing of all your information to be in compliance with the provisions of POPI.

4.7 USING THE COMPANY'S WEBSITE

4.7.1 Information processed when using the Company's website

When using the Company's website, the Company may process the following information:

- your IP address;
- Your contact information;
- Details of the browser or type of device used;
- Any information which you may voluntarily complete;
- Information relating to your use of the Company's website, e.g. time spent on the website, details of the pages which you have visited.

4.7.2 Why the Company processes such information

The Company processes such information to better the Company's services and our website and to customise the Company's website for you based on your preferences.

4.7.3 Cookies and other site data

The Company's website utilises cookies and similar technologies. When you first access the website, the Company will advise you that it utilises cookies and other similar tracking technology. Should you accept the use of such cookies these may be stored on your device.

Cookies are small bits of data created by a web browser when used by you, which tracks and personalises your use of the specific web page to be in line with your preferences. This data is saved on your device to improve your browsing experience. These cookies do not allow the Company to access any information on your device but rather provides the Company with information on how you have used the Company website. This information allows the Company to improve its website to provide you with a better experience.

You may block these cookies in the settings for your web browser. You may also remove the cookies already stored on your device by clearing your browsing history in your web browser, making sure to select the removal of all cookies and other site data. However, blocking or removing cookies may affect the functionality of the Company's website.

4.7.4 Links to other websites

The Company's website may contain links to other sites. The presence of links to other third-party sites are not an endorsement by the Company of such site or the services offered on the third-party site.

While the Company endeavours to only provide links to websites that have privacy and data protection policies which are in line with or more onerous than the Company's policies, the Company does not take any responsibility for the data protection policies implemented on such sites or the services offered thereon.

4.7.5 Marketing and communications

You have the right to choose whether the Company may use your information for the purposes of communicating directly with you for marketing the Company's products and services. If you elect to allow such communications and marketing the Company may contact you by telephone, sms, email or post. You can opt out of such communications and marketing at any time by sending an email to data.protection@scriptholdings.com with the word UNSUBSCRIBE in the Subject field.

4.8 ROLES & RESPONSIBILITIES

4.8.1 Information Officer

Script Technologies has appointed an Information Officer in terms of the Act. The Information Officer will be duly registered with the Information Regulator as is required by the applicable legislation after its establishment.

The Company will also designate where necessary, a Deputy Information Officer. The Deputy Information Officer will also be duly registered with the Information Regulator after establishment as is required, reporting directly to the Information Officer of the Company.

Responsibilities are as follows:

- Ensure a compliance framework is developed, implemented, monitored and maintained;
- Ensure a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

- Develop a manual which is, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA;
- Processes are developed together with adequate systems to process requests for information or access thereto;
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the Company collects, holds, uses, shares, discloses, destroys and processes personal information;
- Ensuring that employees and other persons acting on behalf of the Company are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company's security controls;
- Organising and overseeing the awareness training of employees and other individuals regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator;
- Addressing all PoPIA related requests and complaints made by the Company's data subjects;
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officer will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

If needed a Deputy Information Officer will be appointed and will assist the Information Officer in performing his or her duties.

4.8.2 IT Manager or Delegated Technical Resource

The IT Manager (or delegated technical resource) is responsible for defining, implementing, and maintaining security measures for the Company's ICT systems and Information Security Management.

Key responsibilities include:

- Implementing and maintaining technical security controls and ICT infrastructure;
- Conducting risk analysis and supervising access rights;
- Responding to security threats and incidents;
- Supporting business continuity plans, including backup and disaster recovery;
- Raising user awareness on IT security;
- Ensuring encryption tools are available for secure electronic data transfers;
- Protecting servers, computers, and cloud storage with firewalls and security software;
- Securing cross-border data transfers in compliance with regulations;
- Conducting vulnerability assessments and IT audits to detect unauthorized access;
- Performing due diligence on third-party service providers handling personal data.

4.8.3 Marketing And Communication Manager

The Company's Marketing and Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters;

- Addressing any personal information protection queries from journalists or media outlets such as newspapers; and
- Where necessary, working with persons acting on behalf of the Company to ensure that any outsourced marketing initiatives comply with PoPIA.

In the absence of the role, the Information Officer will fulfil these responsibilities.

4.8.4 Employees and Other Persons Acting on Behalf of the Company

During the performance of duties, employees and other persons acting on behalf of the Company (Data Processors), could have access to the personal information of certain clients, suppliers and other employees. They are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Data Processors may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Company or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Data Processors must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Processing of Personal Information

Employees and authorized representatives of the Company may only process personal information if:

- The data subject (or a legal guardian, if a minor) consents;
- Processing is necessary for contract performance, legal obligations, or the data subject's legitimate interests; or
- Processing is required for the legitimate interests of the Company or an authorized third party.

Prohibited Actions
Employees and representatives must not:

- Access or process personal information unless required for their duties;
- Store personal information on personal devices (e.g., laptops, phones, USBs);
- Share personal information informally or via unencrypted emails;
- Transfer personal information outside South Africa without approval from the Information Officer and Data Subject.

Responsibilities
Employees and representatives must:

- Keep personal information secure and minimize unnecessary storage;
- Encrypt electronic transmissions of personal data (IT support available if needed);
- Use password protection for all devices storing personal information and never share passwords;

- Lock screens and secure removable storage devices when not in use;
- Store hard copies in secure locations and upload electronic data only to approved cloud storage;
- Ensure printed personal data is not left unattended;
- Keep data accurate and up to date, obtaining approval before making changes;
- Retain personal information only as long as necessary and dispose of it securely with approval;
- Undergo regular POPI Awareness training.

Where an employee, or a person acting on behalf of the organization, becomes aware or suspicious of any security breach such as the unauthorized access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer. Facilities to report such breaches are available through emailing the data.protection@scriptholding.com address.

4.9 ACCESS REQUEST PROCEDURE

Any person has the right to request details of information and records held by the Company and to obtain copies of such records and information in accordance with clause 19 of the Information Manual, but subject to the grounds for refusal as provided in PAIA and detailed in clause 20 of the Information Manual.

Where the Company processes any of your information, you may submit a request to the Information Officer to correct or delete such information where the information is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or was obtained unlawfully. Such request must be submitted on prescribed Form 2, which is available on request from the Information Officer.

Should you have any queries regarding the processing of your information by the Company, please contact the Company's information officer ("**Information Officer**"):

Information Officer:	Matthew Swanepoel
Contact number:	011 568 9260
Email:	data.protection@Scriptholdings.com

You can also access the Company's full Information Manual (PAIA) published on the web site. This Information Manual details:

a. the categories of information that the Company holds;
b. how this information is processed by the Company;
c. the manner in which such information may be accessed and grounds for refusal of access to such Information; and
d. the manner of objecting to the processing of information and requesting a correction or deletion of information processed by the Company.

4.9.1 COMPLAINT TO THE INFORMATION REGULATOR

Should you believe that any of your rights to the protection of your information have been violated, you may approach the Information Regulator to submit a complaint.

4.10 ACCOUNTABILITY AND DISCIPLINARY ACTION

Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or non-compliance to the Company's policy prescriptions, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of the Company.

Where the Information Officer together with Management believes that the conduct may constitute a violation of any applicable law, rule, or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

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

The contractual agreements of external third-party contractors to the Company will be subject to immediate suspension or termination in the sole discretion of the senior management of the Company, pending investigation and recommendations of the Information Management Committee of the Company.

4.11 UPDATING OUR POLICY

The Company reserves the right to update the terms of this Data Privacy and Protection Policy and the Information Manual at any time and to publish such updated privacy policy and Information Manual on the Company's website.

You may contact the Information Officer at any time to obtain a copy of the most recent Data Privacy and Protection Policy and PAIA Manual.

5. REFERENCES

Document No/Source	Document Name
POL ISM 003	PAIA Manual
Form 1	Objection to the Processing of Personal Information
Form 2	Request for Access to Information- Regulation 7
Form 2	Request for Correction or Deletion of Personal Information
Form 3	Notice of outcome of request for access to information
Form 4	Obtain Data Subject Consent
FORM HR 003	Employee Personal Information Consent Form
https://popia.co.za/act/	POPI Act
https://www.michalsons.com/	Michalson's Attorneys' website
LSSA (Law Society of South Africa) Guidelines	Protection of Personal Information for South African Law Firms

Document No/Source	Document Name
Information Regulator	Draft Guidelines on the Registration of Information Officers
https://serr.co.za	POPI Act- Obtaining Consent
https://www.tech4law.co.za	Processing Limitations