PAIA MANUAL

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

TANOSEC CYBERSECURITY

Bloemfontein, Free State, South Africa

DATE OF COMPILATION	10 September 2026
DATE OF REVISION	10 September 2026

Public contact: +27 (62) 123 4244 | info@tanosec.co.za | support@tanosec.co.za

Website: https://tanosec.co.za

TABLE OF CONTENTS

1. LIST OF ACRONYMS AND ABBREVIATIONS

Acronym	Meaning
DIO	Deputy Information Officer
IO	Information Officer
PAIA	Promotion of Access to Information Act 2 of 2000, as amended
POPIA	Protection of Personal Information Act 4 of 2013
Regulator	Information Regulator (South Africa)
Republic	Republic of South Africa
Tanosec	Tanosec Cybersecurity

2. PURPOSE OF THIS PAIA MANUAL

This Manual is intended to help members of the public understand what records Tanosec holds, how access to those records may be requested, and how Tanosec processes and protects personal information.

- identify categories of records that may be available without a formal PAIA request;
- understand how to submit a request for access to a record held by Tanosec;
- identify records held in terms of other applicable South African legislation;
- obtain the contact details of the Information Officer;
- understand where to obtain the Information Regulator's PAIA Guide;
- understand the purposes for which Tanosec processes personal information;
- understand the categories of data subjects and personal information processed;
- understand the categories of recipients to whom personal information may be supplied;
- understand possible transborder flows of personal information; and
- understand the general information-security measures used to protect personal information.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION

3.1 Information Officer

Field	Details
Name	Lawrence Lackey
Role	Founder / Head of Tanosec Cybersecurity

Telephone	+27 (62) 123 4244
Email	info@tanosec.co.za
Support email	support@tanosec.co.za

3.2 Deputy Information Officer

No Deputy Information Officer is listed in this Manual. If a Deputy Information Officer is formally designated, the Manual will be updated accordingly.

3.3 General contact for access to information

Requests and enquiries relating to access to information may be sent to info@tanosec.co.za.

3.4 Head office / principal place of business

Field	Details
Business locality	Bloemfontein, Free State, South Africa
Postal address	52 Gascony Crescent, Helicon Heights, Bloemfontein, 9301
Physical / street address	52 Gascony Crescent, Helicon Heights, Bloemfontein, 9301
Telephone	+27 (62) 123 4244
Email	info@tanosec.co.za
Website	https://tanosec.co.za

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

The Information Regulator has made available a Guide on how to use PAIA. The Guide explains the objects of PAIA and POPIA, how to request access to records, available assistance, remedies, fees and related procedures.

The Guide is available from the Information Regulator's website and eServices portal and may also be requested from Tanosec's Information Officer.

Information Regulator	Current contact details
Website	https://inforegulator.org.za
eServices	https://eservices.inforegulator.org.za
Telephone	010 023 5200
Toll-free	0800 017 160
General email	enquiries@inforegulator.org.za
PAIA complaints	PAIAComplaints@inforegulator.org.za
Physical address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
Postal address	P.O. Box 31533, Braamfontein, Johannesburg, 2017

For local accessibility, English and Sesotho versions of the Regulator's PAIA Guide may be consulted. Other official-language versions are available from the Regulator.

5. CATEGORIES OF RECORDS AVAILABLE WITHOUT A FORMAL PAIA REQUEST

The following records are generally available publicly or may be supplied informally without requiring a formal PAIA request, subject to confidentiality, legal restrictions and the nature of the request.

Category of record	Examples	How available
Corporate and public information	Company profile, contact information,	Website / on request

	service descriptions, FAQs	
Policies and notices	Privacy Policy, Terms of Use, Cookie Policy, public notices	Website
Published resources	Insights, guides, reports and downloadable cybersecurity resources	Website
Marketing material	Public newsletters, social-media posts, service brochures	Website / social media / on request
PAIA Manual	Current version of this Manual	Website / on request

6. RECORDS AVAILABLE IN ACCORDANCE WITH OTHER LEGISLATION

Tanosec may create, retain or make records available in accordance with legislation applicable to its activities. The precise legislation applicable to a particular record will depend on Tanosec's legal form, tax status, staffing and the nature of the relevant service or transaction.

Category of records	Applicable legislation (where applicable)
PAIA Manual and access-request records	Promotion of Access to Information Act 2 of 2000
Personal-information and privacy records	Protection of Personal Information Act 4 of 2013
Electronic communications and online transactions	Electronic Communications and Transactions Act 25 of 2002
Cybersecurity incident and cybercrime-related records	Cybercrimes Act 19 of 2020
Tax and accounting records	Income Tax Act 58 of 1962; Tax Administration Act 28 of 2011; Value-Added Tax Act 89 of 1991 where applicable
Corporate records	Companies Act 71 of 2008, if applicable to Tanosec's legal form
Employment records	Basic Conditions of Employment Act 75 of 1997 and other employment legislation, if applicable
Consumer and service-related records	Consumer Protection Act 68 of 2008, where applicable

7. SUBJECTS ON WHICH TANOSEC HOLDS RECORDS AND CATEGORIES OF RECORDS

Subject	Categories of records
Governance and compliance	Policies, PAIA/POPIA compliance records, information-security policies, risk and governance records
Clients and prospects	Enquiries, proposals, quotations, contracts, scopes of work, authorisations, correspondence and support records
Cybersecurity service delivery	Assessment notes, vulnerability findings, penetration-test records, digital-footprint/OSINT findings, phishing-simulation records, awareness-training records, technical evidence and reports
Managed cybersecurity	Monitoring records, alerts, investigation notes, configuration records, asset information, playbooks and service reports
Finance	Invoices, payment records, accounting records, expense and tax records
Service providers and partners	Supplier information, agreements, due-diligence records, technical and commercial correspondence
Website and marketing	Website enquiries, resource downloads, newsletter records, analytics, public content and campaign records
Human resources / contractors	Employment or contractor records, qualifications, onboarding and administrative records, where applicable
Security and incident management	Access logs, security alerts, incident records, evidence, breach-response documentation and recovery records

8. PROCESSING OF PERSONAL INFORMATION

8.1 Purpose of processing personal information

Tanosec processes personal information only where reasonably necessary for legitimate business, contractual, legal, security and service-delivery purposes. These purposes may include:

- responding to enquiries and communicating with prospective and existing clients;
- preparing quotations, proposals, contracts, invoices and service documentation;
- delivering cybersecurity assessments, consulting, managed security, training and related services;
- verifying authorised contacts and maintaining client-account information;
- providing technical support and maintaining service records;
- operating and securing Tanosec's website, systems, endpoints and infrastructure;
- detecting, investigating and responding to security incidents, abuse or fraud;
- meeting legal, regulatory, tax, accounting and record-keeping obligations;
- managing service providers, specialist partners and business relationships; and
- sending marketing or educational communications where permitted by law or consented to.

8.2 Categories of data subjects and personal information

Data subjects	Personal information that may be processed
Prospective and existing clients	Names, contact details, job titles, organisation details, correspondence, service requirements, billing and transaction information
Client personnel / authorised users	Names, work contact details, roles, usernames or technical identifiers, access information supplied for authorised service delivery, and activity relevant to a scoped engagement
Suppliers, partners and contractors	Names, contact details, business details, registration/tax information where relevant, contracts, invoices and payment details
Website visitors and enquirers	IP addresses, device/browser information, analytics data, form submissions, email addresses and communications
Employees / contractors (if applicable)	Identification and contact details, employment/contract records, qualifications, payroll or banking information and other legally required information
Individuals appearing in authorised security investigations	Publicly available information, technical identifiers, account references or other information strictly relevant to a lawful and authorised engagement

8.3 Recipients or categories of recipients

Category of personal information	Recipients or categories of recipients
Client and service-delivery information	Authorised Tanosec personnel, the relevant client, and approved specialist partners where necessary and appropriately authorised
Business administration and financial information	Accounting, payment, banking, tax and professional service providers, as required
Hosted / cloud information	Approved hosting, email, productivity, backup, security and cloud-service providers acting under appropriate contractual or data-protection terms
Legal or regulatory information	The Information Regulator, courts, law-enforcement agencies, regulators or other authorities where disclosure is required or permitted by law
Security incident information	Affected clients, approved incident-response or technical specialists, insurers or authorities where appropriate and lawful

8.4 Planned transborder flows of personal information

Tanosec uses online and cloud-based services. As a result, certain personal information may be stored, backed up or processed outside South Africa by service providers with infrastructure in other countries. Where cross-border processing occurs, Tanosec seeks to apply the safeguards required by section 72 of POPIA and to use service providers with appropriate privacy, security and contractual protections.

The specific country and provider may vary according to the service in use and the client's requirements. Additional detail may be provided where lawfully requested and where disclosure would not create a security risk or breach confidentiality.

8.5 General description of information-security measures

Tanosec applies reasonable technical and organisational safeguards designed to protect the confidentiality, integrity and availability of personal information. Depending on the system and risk, these measures may include:

- access control based on least privilege and role requirements;
- multi-factor authentication and strong authentication controls;
- encryption in transit and encryption at rest where supported and appropriate;
- endpoint hardening, anti-malware and security monitoring;
- patching, vulnerability management and secure configuration practices;
- logging, alerting and review of security-relevant events;
- segmentation and restricted administrative access where appropriate;
- secure backups and recovery procedures;
- confidentiality controls for client data and engagement evidence;
- vendor and service-provider due diligence;
- incident-response and breach-management procedures; and
- secure retention and disposal practices appropriate to the sensitivity of the information.

9. AVAILABILITY OF THE MANUAL

A copy of this Manual is intended to be made available:

- on Tanosec's website at https://tanosec.co.za;
- from the Information Officer upon request;
- for public inspection at Tanosec's principal place of business by prior arrangement during normal business hours;
- to any person upon request, subject to any fee lawfully prescribed for copies; and
- to the Information Regulator upon request or through the Regulator's eServices portal where required.

10. UPDATING OF THE MANUAL

The Information Officer will review this Manual periodically and update it when material changes occur to Tanosec's contact details, records, processing activities, legal obligations or information-security practices.

Issued by:

Lawrence Lackey

Founder / Information Officer