PAIA MANUAL

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

DATE OF COMPILATION: 24/10/2025
DATE OF REVISION: 14/11/2025

info@superworker.co

410 Lynnwood Road,
Lynnwood,
Pretoria,
0081

TABLE OF CONTENTS

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1	**AFS**	Annual Financial Statements
1.2	**AML/ CTF**	Anti-Money Laundering / Counter-Terrorist Financing
1.3	**B-BBEE**	Broad-Based Black Economic Empowerment
1.4	**BCP/ DR**	Business Continuity Planning / Disaster Recovery
1.5	**BO**	Beneficial Ownership
1.6	**CCMA**	Commission for Conciliation, Mediation and Arbitration
1.7	**CEO**	Chief Executive Officer (often the "head" of the private body under PAIA/POPIA)
1.8	**CIPC**	Companies and Intellectual Property Commission
1.9	**COIDA**	Compensation for Occupational Injuries and Diseases Act
1.10	**CPA**	Consumer Protection Act
1.11	**CPD**	Continuing Professional Development
1.12	**DEL**	Department of Employment and Labour
1.13	**DIO**	Deputy Information Officer (assists the IO under PAIA/POPIA)
1.14	**DPIA/ PIA**	Data/Privacy Impact Assessment (not the same as PAIA)
1.15	**ECTA**	Electronic Communications and Transactions Act
1.16	**EE/ EEA**	Employment Equity / Employment Equity Act
1.17	**EMP201**	Monthly Employer Declaration (PAYE/SDL/UIF)
1.18	**EMP501**	Employer Reconciliation Declaration
1.19	**HR**	Human Resources
1.20	**IO**	Information Officer (responsible for PAIA/POPIA compliance)
1.21	**IT**	Information Technology
1.22	**IT3**	Third-party Tax Certificate (e.g., IT3(a))
1.23	**KPI**	Key Performance Indicator
1.24	**KYC**	Know Your Customer
1.25	**Minister**	Minister of Justice and Correctional Services (administers PAIA)
1.26	**MOI**	Memorandum of Incorporation
1.27	**MSA**	Master Services Agreement
1.28	**NDA**	Non-Disclosure Agreement
1.29	**OHS Act**	Occupational Health and Safety Act
1.30	**Operator**	A third-party processor under POPIA
1.31	**PAIA**	Promotion of Access to Information Act, 2000
1.32	**PAYE**	Pay-As-You-Earn
1.33	**PO**	Purchase Order
1.34	**POPIA**	Protection of Personal Information Act, 2013
1.35	**Regulator**	Information Regulator (South Africa)
1.36	**Republic**	Republic of South Africa
1.37	**SaaS**	Software as a Service
1.38	**SAPS**	South African Police Service (Criminal Record Centre)
1.39	**SARS**	South African Revenue Service
1.40	**SAQA**	South African Qualifications Authority
1.41	**SETA**	Sector Education and Training Authority
1.42	**SLA**	Service Level Agreement
1.43	**SoW/ SOW**	Statement of Work
1.44	**UIF**	Unemployment Insurance Fund
1.45	**VAT**	Value-Added Tax
1.46	**WIP**	Work in Progress (project accounting)

2. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to-

2.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request.

2.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject.

2.3 know the description of the records of the body which are available in accordance with any other legislation;

2.4 access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access.

2.5 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it.

2.6 know if the body will process personal information, the purpose of processing personal information and the description of the categories of data subjects and of the information or categories of information relating thereto.

2.7 know the description of the categories of data subjects and of the information or categories of information relating thereto.

2.8 know the recipients or categories of recipients to whom the personal information may be supplied.

2.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

2.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF SUPERWORKER

3.1 Chief Information Officer

Name:	Christo Smit
Tel:	+27 83 297 8483
Email:	christo.smit@vsls.com

3.2 Deputy Information Officer

Name:	Christo Smit
Tel:	+27 83 297 8483
Email:	christo.smit@vsls.com

3.3 Access to information general contacts

Email:	info@superworker.co

3.4 National or Head Office

Postal Address: The Corner Office, 410 Lynwood Road, Pretoria, GP, 0081

Physical Address:The Corner Office, 410 Lynwood Road, Pretoria, GP, 0081

Telephone:	+27 83 297 8483
Email:	info@superworker.co
Website:	https://superworker.co/

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

4.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2. The Guide is available in each of the official languages and in braille.

4.3. The aforesaid Guide contains the description of:

4.3.1. the objects of PAIA and POPIA.

4.3.2. the postal and street address, phone number and, if available, electronic mail address of-

4.3.2.1. the Information Officer of every public body, and

4.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA1 and section 56 of POPIA2.

4.3.3. the manner and form of a request for-

4.3.3.1. access to a record of a public body contemplated in section 113; and

4.3.3.2. access to a record of a private body contemplated in section 504.

4.3.4. the assistance available from the IO of a public body in terms of PAIA and POPIA.

4.3.5. the assistance available from the Regulator in terms of PAIA and POPIA.

4.3.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging:

[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 56(a) of POPIA- Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.*

[3] *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.*

[4] *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.

4.3.6.1. an internal appeal.

4.3.6.2. a complaint to the Regulator; and

4.3.6.3. 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.

4.3.7. the provisions of sections 14[5] and 51[6] requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual.

4.3.8. the provisions of sections 15[7] and 52[8] providing for the voluntary disclosure of categories of records by a public body and private body, respectively.

4.3.9. the notices issued in terms of sections 22[9] and 54[10] regarding fees to be paid in relation to requests for access; and

4.3.10. the regulations made in terms of section 92[11].

[5] *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.*

[6] *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.*

[7] *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*

[8] *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*

[9] *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.*

[10] *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.*

[11] *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."

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

4.5. The Guide can also be obtained-

4.5.1. upon request to the Information Officer.

4.5.2. from the website of the Regulator (https://www.justice.gov.za/inforeg/).

4.6 4.6 A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours-

4.6.1. ENGLISH AND AFRIKAANS

5. CATEGORIES OF RECORDS OF SUPERWORKER WHICH ARE AVLIBLE WITHOUT A PERSON HAVING TO REQUEST ACCESSS

Category of records	Types of the Record	Available on Website	Available upon request
Records Available Without Request	Company profile and brochures	X	X
Records Available Without Request	Company policies (as published)		X
Records Available Without Request	BEE certificate		X
Records Available Without Request	PAIA and POPIA compliance information (as published)	X	X
Personnel Records	Contracts and agreements, contact details, performance reviews		X
Client Records	Contracts and service agreements, correspondence, project documentation		X
Financial Records	Annual financial statements, invoices, tax-related documents		X
Company Records	CIPC documents, board resolutions, shareholder agreements		X
Contractor Records	Independent contractor agreements, NDAs, POPIA acknowledgements		X
Other Records	Internal policies, risk registers, insurance certificates		X

6. DESCRIPTION OF THE RECORDS OF SUPERWORKER WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

Category of Records	Applicable Legislation
Memorandum of Incorporation (MOI)	Companies Act 71 of 2008
CIPC registration documents, name-change certificates, annual returns	Companies Act 71 of 2008 (ss 32-33, including Companies Regulations)
Securities/ beneficial-interest register and beneficial-ownership register/ fillings	Companies Act 71 of 2008 as amended by General Laws (AML/CTF) Amendment Act 22 of 2022, CIPC Beneficial Ownership directives (including filing with annual returns)
Board and shareholder resolutions, minutes of meetings	Companies Act 71 of 2008
Accounting records, financial statements, access to AFS	Companies Act 71 of 2008 (ss 28-31)
Tax records (income tax/ PAYE/ EMP201/ EMP501, IRP5/IT3, provisional tax)	Tax Administration Act 28 of 201, Income Tax Act 58 of 1962
VAT records (returns, invoices, working papers)	Value-Added Tax Act 89 of 1991; Tax Administration Act 28 of 2011
UIF contribution and declarations (e.g., UI-19), employer registration	Unemployment Insurance Contributions Act 4 of 2002, Unemployment Insurance Act 63 of 2001, SARS UIF guidance
Employment contracts, attendance and wage registers, pay slips, leave	Basic Conditions of Employment Act 75 of 1997 and BCEA Regulations (record-keeping)
Disciplinary records	Labour Relations Act 66 of 1995 (Schedule 8 – Code of Good Practice: Dismissal)
Employment Equity plans, EEA reports and related records (if applicable)	Employment Equity Act 55 of 1998 and Regulations
Workplace health and safety records (risk assessments, incidents registers, H&S committee minutes)	Occupational Health and Safety Act 85 of 1993 and Regulations
Compensation for Occupational Injuries & Diseases claims/ accident reports	COIDA 130 of 1993 and Regulations
PAIA Manual	Promotions of Access to Information Act 2 of 2000 (s 51)
PAIA request/ decision/ appeal logs, fee records	PAIA 2 of 2000 (procedural provisions)
POPIA/ Privacy records (Information Officer registration, processing notices/ consents, operator agreements, complaints and breach logs)	Protection of Personal Information Act 4 of 2013 (and Regulations), Information Regulator guidance
Website/ e-commerce supplier disclosures, T&Cs	Electronic Communications and Transactions Act 25 of 2002 (s 43)
Consumer-facing records (direct-marketing/ consents/ opt-outs, cooling-off and cancellations)	Consumer Protection Act 68 of 2008, ECTA 25 of 2002 (for online transactions)
B-BBEE certificate/ affidavit	Broad-Based Black Economic Empowerment Act 53 of 2003 and Codes of Good Practice

7. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY THE BODY

Subjects on which the body holds records	Categories of records
Strategy and governance	Strategic plans, business plans, company-wide policies and procedures
Company secretariat and statutory	MOI, CIPC registrations and annual returns, board/shareholder resolutions and minutes, beneficial-ownership register, shareholder agreements
Finance and tax	Annual financial statements, management accounts and budgets, bank reconciliations, debtor/ creditor ledgers, contract and supplier invoices, purchase orders, payment runs and remittance advices, fixed-asset register, tax returns and working papers (Income Tax, PAYE/EMP201/EMO501)
Human resources (employees)	HR policies, employment contracts and addenda, personal files, onboarding/ exit records, job descriptions, leave and attendance, payroll and remuneration records, disciplinary/ grievance records, training and CPD, EE records (if designated)
Recruitment and talent acquisition (candidates)	Job adverts, applications and CVs, assessment results, interview notes, reference/ background checks and consents, candidate correspondence
Independent contractors and freelancers	Independent contractor/ supplier onboarding forms, tax-compliance PIN, B-BBEE affidavit/ certificate, rate cards/ hourly fee schedules and caps, scopes of work (SOWs)/ purchase orders, timesheets and approvals, deliverable acceptance/ sign-offs, invoices and statements, NDAs, operator/data-processing agreements (POPIA), conflict of interest and independence declarations, proof of professional indemnity/ public-liability insurance, correspondence and performance notes
Timekeeping, billing and project accounting	Timesheets (employees and contractors), allocation to projects/ WI, approval logs, billing schedules and milestones, client Pos, charge-out/ standard rate tables, revenue recognition worksheets
Procurements and supplier management	Supplier diligence/ KYC, SLA/MSA templates, evaluation/ selection records, supplier performance reviews, termination blacklist records
Client engagement and project delivery	Proposals and bids, MSAs/ SLAs/ SOWs, project plans, risk/issue logs, deliverables and reports, meeting notes, change requests, acceptance/ signoffs, client feedback/ surveys, correspondence
Legal and compliance	Contracts templates, NDAs, license/ assignment agreements, PAIA manual, PAIA request/ decision/ fee logs, POPIA processing registers and consents, operator agreements, complaints and dispute files, breach/incident logs, Information Officer registration and correspondence
Risk management and insurance	Enterprise risk register, project risk registers, business-continuity/ disaster-recovery plans, insurance policies and schedules, claims and correspondence
Information technology and security	IT/ security policies, asset inventories, user access records, device assignment/ return forms, backup/change logs, SaaS/ admin audit logs, vendor security assessments, DPIAs/ PIAs
Health, safety and environment (HSE)	H&S policy, risk assessment, incident/ accident registers, COIDA claims, inductions and training records
B-BBEE and transformation	Company B-BBEE certificate/ affidavit, supplier B-BBEE documents used for procurement recognition

Facilities and assets	Office lease and utilities, access control lists, equipment assignment records, maintenance and warranty documents
Knowledge management and methodology	Delivery templates and toolkits, internal standards/ guides, research/ insight notes, training materials
Other corporate records	Internal polices not listed above, insurance certificates, general correspondence, archives and retention schedules

8. PROCESSING OF PERSONAL INFORMATION

8.1 Purpose of Processing Personal Information

Superworker processes personal information to enable the effective delivery of consulting services. This includes:

- Managing relationships with clients and independent contractors.
- Fulfilling contractual and legal obligations.
- Administering payments, invoicing, and tax compliance.
- Ensuring compliance with regulatory requirements, including PAIA and POPIA.
- Protecting legitimate business interests, such as safeguarding confidential information and maintaining security of systems.
- Facilitating communication and service delivery while consulting engagements.

Personal information is only processed where necessary, relevant, and proportionate to the purpose for which it was collected.

8.2 Description of the categories of Data Subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Personal Information that may be processed
Strategy and governance	Strategic plans, business plans, company-wide policies and procedures
Company secretariat and statutory	MOI, CIPC registrations and annual returns, board/shareholder resolutions and minutes, beneficial-ownership register, shareholder agreements
Finance and tax	Annual financial statements, management accounts and budgets, bank reconciliations, debtor/ creditor ledgers, contract and supplier invoices, purchase orders, payment runs and remittance advice, fixed-asset register, tax returns and working papers (Income Tax, PAYE/EMP201/EMO501)
Human resources (employees)	HR policies, employment contracts and addenda, personal files, onboarding/ exit records, job descriptions, leave and attendance, payroll and remuneration records, disciplinary/ grievance records, training and CPD, EE records (if designated)
Recruitment and talent acquisition (candidates)	Job adverts, applications and CVs, assessment results, interview notes, reference/ background checks and consents, candidate correspondence
Independent contractors and freelancers	Independent contractor/ supplier onboarding forms, tax-compliance PIN, B-BBEE affidavit/ certificate, rate cards/ hourly fee schedules and caps, scopes of work (SOWs)/ purchase orders, timesheets and approvals, deliverable acceptance/ sign-offs, invoices and statements, NDAs, operator/data-processing agreements (POPIA), conflict of interest and independence declarations, proof of professional indemnity/ public-liability insurance, correspondence and performance notes
Timekeeping, billing and project accounting	Timesheets (employees and contractors), allocation to projects/ WI, approval logs, billing schedules and milestones, client Pos, charge-out/ standard rate tables, revenue recognition worksheets

Procurements and supplier management	Supplier diligence/ KYC, SLA/MSA templates, evaluation/ selection records, supplier performance reviews, termination blacklist records
Client engagement and project delivery	Proposals and bids, MSAs/ SLAs/ SOWs, project plans, risk/issue logs, deliverables and reports, meeting notes, change requests, acceptance/ sign-offs, client feedback/ surveys, correspondence
Legal and compliance	Contracts templates, NDAs, license/ assignment agreements, PAIA manual, PAIA request/ decision/ fee logs, POPIA processing registers and consents, operator agreements, complaints and dispute files, breach/incident logs, Information Officer registration and correspondence
Risk management and insurance	Enterprise risk register, project risk registers, business-continuity/ disaster-recovery plans, insurance policies and schedules, claims and correspondence
Information technology and security	IT/ security policies, asset inventories, user access records, device assignment/ return forms, backup/change logs, SaaS/ admin audit logs, vendor security assessments, DPIAs/ PIAs
Health, safety and environment (HSE)	H&S policy, risk assessment, incident/ accident registers, COIDA claims, inductions and training records
B-BBEE and transformation	Company B-BBEE certificate/ affidavit, supplier B-BBEE documents used for procurement recognition
Facilities and assets	Office lease and utilities, access control lists, equipment assignment records, maintenance and warranty documents
Knowledge management and methodology	Delivery templates and toolkits, internal standards/ guides, research/ insight notes, training materials
Other corporate records	Internal polices not listed above, insurance certificates, general correspondence, archives and retention schedules

8.3 The recipients or categories of recipients to whom the personal information may be supplied

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Identity number, names, right to work documents	Department of Home Affairs, South African Police Services, clients that require ID for site access (with notice/ consent)
Qualifications, professional registrations	South African Qualifications Authority verification services, education institutions, professional councils, clients that require proof of qualifications
	Credit Bureaus and results shared only with client where legally/ contractually required and with consent
Credit and payment history, for	Clients and prospective clients (project delivery, coordination), supplier/ couriers/ event organisers (logistics), IT service providers supporting communication tools
credit information	Clients (for proposals/ staffing with consent), background-screening vendors, referees you contact for references
Contact details (work email/ phone), job title, employer	Payroll provider, external auditors, legal advisors (if needed), CCMA/ courts when required by the law

Candidate CVs, applications, interview notes, assessments	Bank/ payment processors, payroll provider, SARS (PAYE submissions), external auditors
Employee HR records (contracts, performance, leave)	SARS (income tax, PAYE, VAT if registered), external tax practitioners/ auditors
Payroll, bank details, remuneration	Department of Employment and Labor/ UIF, relevant SETA (for SDL/ skills reporting)
Tax numbers and tax records	Clients (for billing/ verification), accounting system provider, external auditors
UIF/ SDL contribution records	Clients (to evidence resourcing/ rates where required), banks/ payment processors, B-BBEE verification agency (as supplier evidence) external auditors
Timesheets (employees and independent contractors) approvals, billing data	Clients and counterparties, legal advisors, insurers (if required for claims), auditors
Independent contractor data (ID/ company registration, bank, rate cards, SOWs, invoices)	SANAS-accredited B-BBEE verification agencies, clients' procurement teams (on request)
Contracts, NDAs, MSAs, SOWs containing personal information	CIPC (filings with annual returns), auditors, banks when required for KYC
B-BBEE affidavits/ certificates (companies and suppliers)	Compensation Fund (COIDA), insurers/ brokers, client HSE representatives where site rules require it
Beneficial-ownership and director details	Insurers and insurance brokers, loss adjusters/ assessors
Health and safety/ incident reports, medical certificates (limited)	Legal advisors, mediators/ arbitrators, CCMA, courts/ tribunals, law enforcement on request

8.4 Planned transborder flows of personal information

System / recipient category	Purpose	Country / region	Categories of personal information	Legal basis & safeguards (POPIA s72)
Cloud email, identity and collaboration (e.g., Microsoft 365: Exchange, SharePoint, OneDrive, Teams)	Email, file storage, chat and collaboration	EU/UK primary, may include USA for telemetry/ support depending on provider	Client contacts, project documents and deliverables, employee HR docs, candidate CVs and interviews, contractor agreements, timesheets and invoices, corporate records	Contractual necessity, operator agreement, SCCs/UK IDTA (as applicable), access controls and encryption
Video meetings and recordings (e.g., Teams/Zoom)	Meetings, webinars, optional recordings	EU/UK, may include USA	Names, work email, meeting metadata, optional audio/video recordings (with notice/consent)	Consent where recorded, operator agreement, SCCs/UK IDTA
CRM / proposals / e-signature (e.g., CRM, DocuSign/Adobe Sign)	Sales pipeline, proposals, contracting	EU/UK/USA (per vendor residency)	Client/stakeholder contact details, proposals, contracts containing names/signatures	Contractual necessity, operator agreement, SCCs/UK IDTA
Background-screening and verification vendors	ID, qualification, criminal/ credit checks (role-dependent)	South Africa and, where required by vendor/ workflow, EU/UK/USA	ID numbers, names, qualifications, criminal/credit results (only where lawful and consented)	Consent and/or legal obligation, accredited vendors, operator agreement, "adequate protection" assessment

Payroll and HRIS (cloud)	Payroll, leave, payslips, HR records	South Africa and/or EU/UK	Employee identifiers, bank details, tax/PAYE numbers, remuneration, leave data	Legal obligation/ contractual necessity, operator agreement, SCCs/UK IDTA (if cross-border)
Cloud accounting and billing (e.g., invoicing/AP-AR)	Invoicing, AR/AP, audit support	EU/UK and/or USA/Australia (per vendor), with multi-region backups	Client billing data, invoices, contractor invoices, limited bank details for payments	Contractual necessity, legal obligation, operator agreement, SCCs/UK IDTA
Timekeeping and project accounting (e.g., timesheet tools)	Timesheets, approvals, WIP, billing	EU/UK/USA	Names, project identifiers, hours worked, rates (where applicable)	Contractual necessity, operator agreement, SCCs/UK IDTA
Website hosting, CDN and analytics (e.g., managed hosting, CDN, analytics)	Website hosting, DDoS protection, analytics/ cookies	EU/UK/USA (per host/CDN/ analytics)	Contact-form submissions, IP/device data, cookie IDs, marketing preferences	Consent for cookies/marketing and/or legitimate interests, operator agreement, SCCs/UK IDTA
Ticketing/ support and project collaboration (e.g., Jira/Asana/Trello/Zendesk)	Task/issue tracking, client support	EU/UK/USA	Names, work emails, task/support content which may include personal info	Contractual necessity, operator agreement, SCCs/UK IDTA
Cloud backups and disaster recovery (provider sub-processors)	Continuity, data resilience	EU/UK/USA (per provider sub-processor list)	Backup copies of the systems above	Legitimate interests, operator agreement, SCCs/UK IDTA, encryption at rest/in transit
Clients located outside South Africa	Delivery of consulting services	Client locations (e.g., EU/UK/USA)	Candidate CVs and profiles (with consent), project outputs containing contact details, time/billing summaries	Contractual necessity, confidentiality undertakings, secure transfer measures
Insurers and brokers (multinational groups)	Professional-indemnity cover, claims handling	South Africa and EU/UK	Policy/claim information that may include personal info	Legitimate interests/legal obligation, operator agreement, SCCs/UK IDTA (if applicable)
External auditors, tax practitioners and legal counsel (some with foreign affiliates)	Audit, tax compliance, legal advice	South Africa; may include EU/UK	Records containing personal info only as necessary for the mandate	Legal obligation/ privilege, operator agreement, SCCs/UK IDTA (if applicable)

8.5 General description of Information Security Measures to be implemented by the party responsible to ensure the confidentiality, integrity and availability of the information

The company implements appropriate, reasonable technical and organisational measures to ensure the confidentiality, integrity and availability of personal information, consistent with POPIA (including sections 19–22) and our PAIA/POPIA policies. Measures apply to employees and independent contractors with access to our systems.

1) Governance and people controls

- Roles and accountability: Information Officer (IO) and, where appointed, Deputy Information Officer (DIO) oversee security and privacy, managers are accountable for safeguarding on their projects.
- Policies and NDAs: Information Security, Acceptable Use, Remote-work, Password, Clear-desk, and Data Protection policies, all staff/contractors sign confidentiality and (where relevant) operator/data-processing agreements.
- Screening and least access: Role-appropriate background checks (with consent). Access is based on least privilege and need-to-know.

- Training and awareness: Security and POPIA training at onboarding and annually

2) Access and identity management

- Strong authentication: Multi-factor authentication (MFA) for email, VPN/SSO and admin functions.
- Joiner-mover-leaver process: Time-bound accounts for contractors, prompt de-provisioning on exit, periodic access reviews.
- Password hygiene: Minimum length/complexity, change on compromise, password manager recommended, privileged accounts separated.

3) Data classification and handling

- Classification: Public / Internal / Confidential / Personal / Special Personal (e.g., health notes on sick leave, criminal/credit checks).
- Handling rules: Use only approved systems, limit downloads, no sharing to personal email, secure redaction before disclosure, anonymise/pseudonymise where feasible (e.g., candidate shortlists).

4) Encryption and secure communications

- In transit: TLS for email, file transfer, web apps and APIs.
- At rest: Provider-level encryption for cloud storage and backups, full-disk encryption on company laptops.
- Email/file sharing: Use approved secure links with expiry and access controls, encrypt/zip sensitive attachments when links aren't possible.

5) Endpoint and mobile security

- Anti-virus / anti-malware / EDR on laptops, automatic updates and patch management.
- Device management (MDM): Screen-lock, inactivity timeouts, drive encryption, remote-wipe for lost/stolen devices, block or control removable media.
- Admin rights limited; standard users for day-to-day work.

6) Cloud, network and application security

- Secure configuration: Baseline hardening of Microsoft 365/other SaaS (e.g., conditional access, safe links/attachments, restricted external sharing).
- Logging and monitoring: Sign-in and admin activity logs retained, alerting on suspicious access, quarterly review of audit logs.
- Vulnerability management: Regular patching; third-party fixes tracked, high-risk issues remediated promptly.
- Backups and continuity: Point-in-time restore for cloud storage, periodic offline/immutable backups for critical data, BCP/DR plan with restore tests.

7) Vendor, operator and transborder safeguards

- Due diligence: Assess security posture of service providers (cloud, payroll, screening vendors).
- Contracts: Operator agreements include confidentiality, breach-notification and deletion/return-on-termination clauses.

- Cross-border transfers: Where data flows outside South Africa (see "Planned transborder flows"), transfers rely on s72 POPIA bases (e.g., contractual necessity, SCCs/UK IDTA, or consent) and are limited to the minimum necessary.
- Sub-processors: We review providers' published sub-processor lists.

8) Physical and environmental security

- Controlled office access (keys/cards), locked storage for files/devices, and secure shredding of paper records.

9) Records management, retention and disposal

- Data minimisation up front, retention schedules aligned to law (e.g., tax/employment).
- Secure destruction: Certified wiping of drives, deletion workflows in SaaS, documented disposal of paper and media.

10) Incident response and breach notification

- IR plan: Defined steps for identification, containment, eradication, recovery and lessons learned, single incident register.
- Breach notification: Security compromises are assessed and, where required by POPIA s22, reported to the Information Regulator and affected data subjects as soon as reasonably possible, with relevant details and guidance.
- Testing: Table-top exercises at least annually.

Measure	What it does	Where applied
MFA & SSO	Blocks unauthorised access	Email, collaboration, admin portals
Role-based access & reviews	Limits data exposure	Files, CRM, HR, finance systems
Encryption in transit/at rest	Protects data if intercepted/lost	Email, cloud storage, backups, laptops
Endpoint Protection and MDM	Stops malware/data loss	Company and contractor laptops/phones
Secure file sharing	Prevents oversharing	Client deliveries, candidate packs
Backups and DR tests	Ensures availability/recovery	Core SaaS, finance/HR data
Logging and alerting	Detects misuse	M365/SaaS admin and sign-in logs
Vendor DPA/operator clauses	Extends safeguards to third parties	Cloud, payroll, screening vendors
Retention and secure disposal	Reduces risk/obligation	HR, finance, project archives
Training and NDAs	Lowers human error risk	All staff and independent contractors
Incident response and s22 process	Limits harm and ensure compliance	All systems and processes

9. AVAILABILITY OF THE MANUAL

9.1 A copy of the Manual is available-

9.1.1 On https://superworker.co/ if any.

9.1.2 head office of the Superworker for public inspection during normal business hours.

9.1.3 to any person upon request and upon the payment of a reasonable prescribed fee; and

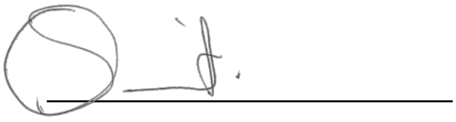
9.1.4 to the Information Regulator upon request.

9.2 A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

10. AVAILABILITY OF THE MANUAL

The head of Superworker will update this manual on a regular basis.

Issued by



Christo Smit

Chief Executive Officer