Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

TARSUS DISTRIBUTION (PTY)LTD

POPIA POLICY:

This document is prepared solely for the private use of Tarsus Distribution (PTY) Ltd management.

It may not be disclosed to any third party without prior written consent from Tarsus Distribution (PTY) Ltd.

Version 1.1 | Approval Date: Sept 2026 | Next Review Date: Sept 2027
Owner | Pearl Masango, General Lead - Compliance, Customer and Risk
Approved by: Rene Du Plessis, General Manager – Legal, Compliance, Risk, Debtors & HR

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Table of Contents

REVISION HISTORY 2
1. GLOSSARY OF TERMS 3
1.1 TERMINOLOGY 3
1.2 ABBREVIATIONS 5
2. INTRODUCTION AND PURPOSE 5
3. SCOPE AND APPLICABILITY 5
4. APPLICABLE DATA PROTECTION LAWS AND REGULATORY FRAMEWORK 6
5. POPIA GOVERNANCE AND ACCOUNTABILITY 6
5.1 BOARD / GORVERNANCE OVERSIGHT 6
5.2 INFORMATION OFFICER 6
5.3 DEPUTY INFORMATION OFFICER 7
5.4 POPIA ADMINISTRATION OFFICER 7
5.5 BUSINESS AND PROCESS OWNERS 7
5.6 INFORMATION TECHNOLOGY AND INFORMATION SECURITY 8
5.7 HUMAN RESOURCES 8
5.8 LEGAL AND COMPLIANCE 8
5.9 EMPLOYEES AND REPRESENTATIVES 8
6. POPIA CONDITIONS FOR LAWFUL PROCESSING 8
7. SPECIAL PERSONAL INFORMATION AND CHILDREN'S PERSONAL INFORMATION 9
8. DATA SUBJECT RIGHTS AND REQUESTS 9
9. TRANSPARENCY AND PRIVACY NOTICES 9
10. PERSONAL INFORMATION PROCESSING ACTIVITIES AND DATA INVENTORY 9
11. PURPOSE SPECIFICATION, FURTHER PROCESSING AND DATA MINIMISATION 10
12. INFORMATION QUALITY AND ACCURACY 10
13. SECURITY SAFEGUARDS 10
14. PERSONAL INFORMATION SECURITY COMPROMISES AND DATA BREACH MANAGEMENT 10
15. OPERATORS AND THIRD-PARTY SERVICE PROVIDERS 11
16. CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION 11
17. DIRECT MARKETING 11
18. DATA RETENTION AND SECURE DISPOSAL 12
19. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS 12
20. RECORDS, DOCUMENTATION AND EVIDENCE 12
21. EMPLOYEE AND WORKPLACE PERSONAL INFORMATION 12
22. CUSTOMER, RESELLER, SUPPLIER AND THIRD-PARTY PERSONAL INFORMATION 13
23. TRAINING AND AWARENESS 13
24. MONITORING, COMPLIANCE AND ASSURANCE 13

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

25. MANAGEMENT REPORTING AND KEY PERFORMANCE INDICATORS 13
26. NON-COMPLIANCE, EXCEPTIONS AND DISCIPLINARY ACTION 13
27. COMPLAINTS AND REGULATORY ENGAGEMENT 14
28. POLICY REVIEW 14
29. RELATED POLICIES, STANDARDS AND PROCEDURES 14
30. CONTACT INFORMATION AND GOVERNANCE RESPONSIBILITIES 14
30.1 GOVERNANCE RESPONSIBILITIES 14
30.2 CONTACT INFORMATION 15

REVISION HISTORY

This Policy shall be subject to formal document control. Changes may be proposed by the Policy Owner, Information Officer, Legal, Compliance, Risk, HR, IT or other relevant stakeholders.

Material changes shall be reviewed by the Information Officer and relevant control owners and approved by the designated approval authority.

Previous approved versions shall be retained in accordance with Tarsus's document retention requirements and shall not be overwritten or retrospectively amended.

Version	Author	Approved by	Summary of Changes	Date Issued	Next Review
V0.1	N Rossouw	A Herbst H Liebenberg	Initial Policy	18 May 2022	TBA
V0.2	C Daffue	G Pickford Rene Du Plessis	Review and Updates	25 Sep 2024	25 Sep 2025
V0.3	C Daffue	Rene Du Plessis Emile Burger	Review and updated details for new CEO	August 2025	August 2026
V1.0	P Masango	Rene Du Plessis	Comprehensive policy review and enhancement to strengthen POPIA governance, accountability and operational requirements	August 2026	August 2027

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Version	Author	Approved by	Summary of Changes	Date Issued	Next Review
V1.1	Legal, Compliance and Risk Department	Rene Du Plessis	Amendments following review.	September 2026	September 2026

Document Control

This Policy shall be approved by the designated governance authority of Tarsus

Policy Approval

By approving this Policy, the designated approving authority confirms that Tarsus Distribution (PTY) Ltd has established a framework for the responsible and lawful processing and protection of personal information.

Title	Name	Signature
General Manager: Legal Compliance, Risk & Debtors & HR	Rene Du Plessis	Signed by: Rene Du Plessis 4AD52702D659469...
General Lead - Compliance, Customer and Risk	Pearl Masango	Signed by: Pearl Masango 969E9C046ABC4C8...
Chief Financial Officer	Anthony Roberts	Signed by: 76E80B3363B542D...

1. GLOSSARY OF TERMS

1.1 TERMINOLOGY

Terminology	Definition
Accountability	The responsibility of Tarsus to ensure and demonstrate that personal information is processed in accordance with applicable data protection requirements.
Board	The Board of Directors of Tarsus Distribution (PTY) Ltd, responsible for overseeing strategic compliance.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Terminology	Definition
Company /Tarsus	Tarsus Distribution (PTY) Ltd, the entity responsible for this Data Protection Policy.
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information, where consent is the applicable lawful basis.
Data Breach / Personal Information Security Compromise	Any unauthorized access, acquisition, disclosure, loss, destruction or compromise of personal information, or any incident that may compromise confidentiality, integrity or availability of personal information.
Data Subject	An identifiable, living natural person and, where applicable under POPIA, an identifiable existing juristic person to whom personal information relates.
Data Subject Request	A request made by a data subject to exercise a right available under applicable data protection law.
Deputy Information Officer	A person appointed in accordance with applicable law to support the Information Officer and manage delegated privacy and information compliance responsibilities.
Information Officer	The person appointed by Tarsus who is responsible for overseeing compliance with applicable information protection and access-to-information obligations.
Operator	A person or organisation that processes personal information for or on behalf of Tarsus in terms of a mandate, without coming under the direct authority of Tarsus.
Personal Information	Information relating to an identifiable, living natural person and, where applicable, an identifiable existing juristic person.
Processing	Any operation or activity concerning personal information, including collection, recording, organisation, storage, updating, retrieval, use, disclosure, transmission, restriction, deletion or destruction.
Privacy Impact Assessment (PIA)	A documented assessment is used to identify, evaluate and mitigate privacy and data protection risks associated with a processing activity, system, project, product, service or technology.
POPIA	Protection of Personal Information Act 4 of 2013, as amended, and applicable regulations.
Responsible Party	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.
Special Personal Information	Personal information falling within the categories identified as special personal information under POPIA, including information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behavior, subject to applicable legal definitions and exceptions.
Third Party	Any person or organisation other than the data subject, Tarsus or an authorized Operator involved in or receiving personal information from Tarsus.
Cross-Border Transfer	The transfer or making available of personal information to a recipient or processing environment outside the Republic of South Africa.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

1.2 ABBREVIATIONS

Abbreviation	Meaning
CEO	Chief Executive Officer
DIO	Deputy Information Officer
GDPR	General Data Protection Regulation
HR	Human Resources
ICT	Information and Communication Technology
ISO	International Organization for Standardization
PAIA	Promotion of Access to Information Act 2 of 2000
PIA	Privacy Impact Assessment
POPIA	Protection of Personal Information Act 4 of 2013
RMCP	Risk Management and Compliance Programme
DPA	Data Processing Agreement

2. INTRODUCTION AND PURPOSE

Tarsus Distribution (PTY) Ltd ("Tarsus" or "the Company") recognizes the importance of protecting personal information entrusted to it by customers, resellers, suppliers, employees, prospective employees, directors, shareholders, service providers and other data subjects.

Tarsus is committed to processing personal information lawfully, responsibly, transparently and securely and to complying with the Protection of Personal Information Act 4 of 2013 ("POPIA") and other applicable data protection requirements.

The purpose of this Policy is to establish Tarsus's framework for the responsible processing and protection of personal information and to:

- establish accountability for the processing of personal information;
- define the principles governing the processing of personal information;
- protect personal information against unauthorized access, use, disclosure, alteration, loss or destruction;
- establish requirements for lawful and responsible processing;
- protect the rights of data subjects;
- establish governance and oversight responsibilities;
- manage personal information security compromises;
- establish requirements for Operators and third parties;
- manage cross-border transfers;
- support privacy-by-design and privacy-by-default;
- establish appropriate retention and secure disposal practices; and
- provide a framework for monitoring and demonstrating compliance.

3. SCOPE AND APPLICABILITY

This Policy applies to Tarsus Distribution (PTY) Ltd, all employees and temporary employees, directors and officers, contractors and consultants, interns and learners, prospective employees, customers and resellers,

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

suppliers and service providers, Operators processing personal information on behalf of Tarsus, third parties who receive personal information from Tarsus, and any other person acting under the authority or instruction of Tarsus.

This Policy applies to personal information processed electronically, manually, in physical records, through business applications and systems, cloud-based services, email and collaboration platforms, websites and digital channels, customer and reseller onboarding processes, credit and risk assessment processes, HR and employee processes, and any other business activity involving personal information.

The Policy applies throughout the personal information lifecycle, from collection through use, storage, disclosure, retention and secure disposal.

4. APPLICABLE DATA PROTECTION LAWS AND REGULATORY FRAMEWORK

Tarsus shall comply with applicable data protection and privacy laws relevant to its processing activities.

The primary South African framework is the Protection of Personal Information Act 4 of 2013 (POPIA), POPIA Regulations, and applicable guidance and regulatory requirements issued by the Information Regulator.

Depending on the nature and location of processing activities, additional laws may apply. Tarsus's operations and data flows involving other jurisdictions may require consideration of applicable local data protection requirements, including requirements applicable in countries in which Tarsus operates or to which personal information is transferred.

The current Policy recognizes the potential relevance of South African POPIA; the European Union General Data Protection Regulation (GDPR), where applicable; the Data Protection Act 13 of 2004 (Mauritius), where applicable; and other applicable data protection laws.

Legal/Compliance shall maintain a current register of jurisdictions and data protection laws applicable to Tarsus's operations and processing activities.

Where different legal requirements apply, the relevant Legal/Compliance function shall determine the applicable requirements and required controls.

5. POPIA GOVERNANCE AND ACCOUNTABILITY

Tarsus shall maintain clear accountability for the protection of personal information.

5.1 BOARD / GORVERNANCE OVERSIGHT

The Board or designated governance structure shall provide appropriate oversight of material privacy and information protection risks.

5.2 INFORMATION OFFICER

The Information Officer is ultimately accountable for Tarsus Distribution's compliance with POPIA and shall provide executive oversight of the Company's privacy and information protection framework.

The Information Officer shall:

- provide strategic oversight of POPIA compliance;

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

- approve privacy policies, standards and governance requirements;
- ensure that appropriate resources are available to support compliance;
- oversee the performance of the Deputy Information Officer and POPIA Administration function;
- report material privacy risks and significant incidents to Executive Management and, where applicable, the Board;
- liaise with the Information Regulator where required by legislation; and
- ensure that Tarsus maintains an effective privacy governance framework.

Note: The Information Officer may delegate operational responsibilities to the Deputy Information Officer and POPIA Administration Officer but retains overall accountability in terms of POPIA.

5.3 DEPUTY INFORMATION OFFICER

The Deputy Information Officer supports the Information Officer by overseeing the operational implementation of the POPIA compliance programme and ensuring that appropriate privacy controls are maintained across the business.

Responsibilities include:

- overseeing implementation of this Policy;
- providing management oversight of privacy compliance activities;
- reviewing significant data subject requests and privacy incidents;
- monitoring compliance reporting and remediation activities;
- supporting regulatory engagements where required;
- providing guidance to business units; and
- escalating significant privacy risks to the Information Officer

5.4 POPIA ADMINISTRATION OFFICER

The POPIA Administration Officer is responsible for the day-to-day administration and coordination of Tarsus Distribution's privacy compliance programme and supports both the Information Officer and Deputy Information Officer.

Responsibilities include:

- maintaining the POPIA compliance framework and supporting documentation;
- drafting, reviewing and updating POPIA policies, procedures and standards;
- maintaining the Personal Information Processing Register and other privacy records;
- coordinating Data Subject Requests and maintaining the request register;
- maintaining the Personal Information Breach Register and coordinating breach investigations;
- coordinating privacy risk assessments and Privacy Impact Assessments (PIAs);
- monitoring compliance with POPIA requirements across business processes;
- coordinating employee POPIA awareness and training initiatives;
- maintaining evidence of compliance for audit and regulatory purposes;
- coordinating Operator and third-party privacy documentation;
- preparing POPIA compliance reports and management information;
- monitoring corrective actions arising from audits, risk assessments and compliance reviews; and
- performing any other administrative duties necessary to support the effective operation of the POPIA compliance programme.

5.5 BUSINESS AND PROCESS OWNERS

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Business and process owners are accountable for ensuring that personal information within their areas of responsibility is processed in accordance with this Policy.

They shall identify personal information processed within their processes; ensure that processing has a defined purpose; ensure appropriate access controls; maintain data quality; comply with retention requirements; identify privacy risks; report incidents; support data subject requests; and ensure that privacy controls are embedded into business processes.

5.6 INFORMATION TECHNOLOGY AND INFORMATION SECURITY

IT and Information Security shall implement appropriate technical safeguards, including, where applicable: access controls; authentication; encryption; secure configuration; vulnerability management; endpoint security; backup and recovery; monitoring and logging; secure disposal; incident response; and other appropriate technical measures.

5.7 HUMAN RESOURCES

HR shall ensure appropriate privacy controls over employee and prospective employee personal information, including recruitment, onboarding, employment records, performance management, payroll, benefits and termination processes.

5.8 LEGAL AND COMPLIANCE

Legal and Compliance shall provide guidance on applicable legal requirements, support risk assessments, review relevant contracts and assist with regulatory engagement and interpretation of privacy obligations.

5.9 EMPLOYEES AND REPRESENTATIVES

All employees and representatives shall comply with this Policy; only access personal information required for their duties; protect confidential information; not disclose personal information without authority; report suspected breaches immediately; complete required training; and comply with applicable information security requirements.

6. POPIA CONDITIONS FOR LAWFUL PROCESSING

Tarsus shall only process personal information where there is a lawful basis for doing so.

Depending on the circumstances, processing may be justified where: the data subject consents; processing is necessary to perform or enter into a contract; processing is necessary to comply with a legal obligation; processing protects a legitimate interest of the data subject; processing is necessary to protect the legitimate interests of Tarsus or a third party, where permitted by law; processing is necessary to perform a public-law duty; or another lawful ground under applicable legislation applies.

Consent shall not be relied upon where another lawful basis is more appropriate, and consent shall not be treated as freely given where the data subject is not able to meaningfully exercise a choice.

Where consent is relied upon, Tarsus shall maintain evidence of consent where required and shall provide an appropriate mechanism for withdrawal.

Withdrawal of consent shall not affect processing lawfully undertaken before withdrawal.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

7. SPECIAL PERSONAL INFORMATION AND CHILDREN'S PERSONAL INFORMATION

Special personal information shall only be processed where permitted by POPIA or other applicable law.

Enhanced safeguards shall be applied where processing involves sensitive or high-risk information.

Children's personal information shall only be processed where permitted under applicable law and appropriate safeguards are in place.

8. DATA SUBJECT RIGHTS AND REQUESTS

Tarsus recognizes the rights available to data subjects under POPIA and applicable law.

Depending on the circumstances, data subjects may have rights relating to: access to personal information; correction or updating of inaccurate information; objection to certain processing; withdrawal of consent where consent is the lawful basis; objection to direct marketing; complaint regarding processing; and other rights provided by applicable law.

Requests shall be directed to the Information Officer or Deputy Information Officer through the approved contact channels.

Tarsus shall: verify the identity of the requester where appropriate; record the request; assess the request; determine whether any lawful grounds for refusal or limitation apply; respond within applicable statutory timelines; maintain appropriate records; and escalate complex or high-risk requests to Legal/Compliance.

Tarsus shall establish and maintain a formal Data Subject Request Procedure.

The designated email address and process for submitting data subject requests.

9. TRANSPARENCY AND PRIVACY NOTICES

Tarsus shall provide appropriate information to data subjects regarding the collection and processing of their personal information.

Privacy notices shall, where applicable, explain: who Tarsus is; what information is collected; why it is collected; the lawful basis for processing; how information is used; who information may be shared with; whether information is transferred internationally; retention considerations; data subject rights; how to contact Tarsus; and how complaints may be lodged.

Tarsus shall maintain and periodically review privacy notices applicable to customers/resellers; suppliers; employees; prospective employees; website users; visitors; marketing recipients; and other relevant data subjects.

10. PERSONAL INFORMATION PROCESSING ACTIVITIES AND DATA INVENTORY

Tarsus shall maintain an appropriate record of significant personal information processing activities.

The record should identify, where applicable: process name; business owner; purpose; categories of data subjects; categories of personal information; special personal information; source of information; lawful basis; systems used; recipients; Operators; retention period; cross-border transfers; security controls; and identified privacy risks.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

The current status, owner and system used to maintain Tarsus's Personal Information/Data Processing Register.

11. PURPOSE SPECIFICATION, FURTHER PROCESSING AND DATA MINIMISATION

Personal information shall only be collected for specific, explicitly defined and lawful purposes related to Tarsus's business activities.

Tarsus shall collect only information reasonably required for the intended purpose; avoid unnecessary collection; not use information for incompatible purposes without appropriate justification; assess proposed secondary uses; ensure data subjects are appropriately informed; and apply appropriate safeguards to further processing.

Any new use of personal information that is materially different from the original purpose shall be assessed by the relevant business owner and, where appropriate, Legal/Compliance or the Information Officer.

12. INFORMATION QUALITY AND ACCURACY

Tarsus shall take reasonably practicable steps to ensure that personal information is accurate, complete, not misleading and updated where necessary.

Business owners shall establish appropriate mechanisms to correct inaccurate information.

Data subjects may request correction or updating of their information in accordance with applicable law.

13. SECURITY SAFEGUARDS

Tarsus shall implement appropriate technical and organizational safeguards to protect personal information against loss; damage; unauthorized destruction; unlawful access; unauthorized processing; alteration; disclosure; and other forms of misuse.

Security safeguards shall be proportionate to the nature and sensitivity of the information and the risk associated with the processing.

Controls may include: role-based access; least-privilege principles; authentication and access management; encryption where appropriate; secure data transmission; endpoint security; malware protection; backups; physical security; secure disposal; monitoring and logging; incident management; employee awareness; and periodic control reviews.

14. PERSONAL INFORMATION SECURITY COMPROMISES AND DATA BREACH MANAGEMENT

Any employee or third party who becomes aware of an actual or suspected personal information security compromise shall report the incident immediately through the approved incident reporting channel.

The response process shall include: identification and reporting; initial assessment; containment; preservation of evidence; investigation; risk assessment; remediation; regulatory notification where legally required; data subject notification where legally required; documentation; and post-incident review.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Operators shall notify Tarsus without undue delay upon becoming aware of a personal information security compromise affecting information processed on Tarsus's behalf.

Notification timelines shall be determined in accordance with POPIA and other applicable law. The current policy's reference to a blanket 72-hour notification requirement shall not be applied automatically to all POPIA incidents, as notification obligations and timelines must be assessed under the applicable legal framework.

Internal breach reporting channel; incident response owner; breach severity classification; regulatory notification approval process; data subject notification process; and breach register owner.

15. OPERATORS AND THIRD-PARTY SERVICE PROVIDERS

Tarsus shall conduct appropriate due diligence before appointing third parties that process personal information on its behalf.

Where required, contractual arrangements shall address: permitted processing; confidentiality; security safeguards; access controls; breach notification; assistance with data subject requests; sub-processing; audit or assurance rights; return or deletion of information; retention; cross-border transfers; and termination obligations.
Operators shall only process personal information in accordance with Tarsus's instructions and applicable law.

Where an Operator or third party will access, receive or process personal information, an appropriate non-disclosure agreement or equivalent confidentiality undertaking must be in place before any personal information is shared. Where financial or commercially sensitive information is to be shared, the applicable Group financial NDA must be used.

16. CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

Tarsus shall assess cross-border transfers of personal information before information is transferred or made available outside South Africa.

Transfers shall only take place where permitted under applicable law and where appropriate safeguards are implemented.

The assessment shall consider: destination country; recipient; purpose; categories of information; data subject categories; legal basis; applicable transfer mechanism; contractual safeguards; security safeguards; and onward transfers.

Where Tarsus operates across South Africa, Namibia, Botswana or other jurisdictions, applicable local data protection requirements shall be considered..

17. DIRECT MARKETING

Tarsus shall conduct direct marketing in accordance with POPIA and other applicable laws.

Marketing activities involving personal information shall be appropriately managed to ensure that: lawful requirements are met; consent is obtained where required; existing customer relationships are managed appropriately; opt-out mechanisms are provided; objections are recorded; suppression lists are maintained; marketing preferences are respected; and personal information is not used for incompatible marketing purposes.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

18. DATA RETENTION AND SECURE DISPOSAL

Personal information shall not be retained for longer than is necessary for the purpose for which it was collected or as required or permitted by law.

Retention periods shall take into account: applicable legislation; contractual obligations; regulatory requirements; tax requirements; employment requirements; FICA requirements where applicable; litigation or legal holds; business requirements; and legitimate operational needs.

Tarsus shall maintain an appropriate Data Retention Schedule.

Personal information that is no longer required shall be securely deleted, destroyed, anonymized or otherwise disposed of in accordance with applicable requirements.

19. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

Privacy considerations shall be incorporated into the design and implementation of new processes, systems, products, services and technologies.

A Privacy Impact Assessment shall be considered where processing may create heightened privacy risks, including: processing of Special Personal Information; large-scale processing; new technologies; AI or automated decision-making; profiling; biometric information; monitoring or surveillance; significant changes to processing; new systems; new cloud services; significant cross-border transfers; or other high-risk processing.

PIAs shall identify: the processing activity; purpose; personal information involved; risks; affected data subjects; safeguards; residual risk; responsible owner; and required remediation.

20. RECORDS, DOCUMENTATION AND EVIDENCE

Tarsus shall maintain appropriate evidence to demonstrate compliance with this Policy and applicable privacy requirements.

Records may include privacy policies; privacy notices; data processing registers; Operator agreements; data subject requests; consent records; breach records; PIAs; training records; risk assessments; audit reports; remediation actions; regulatory correspondence; and management reporting.

Records shall be retained in accordance with applicable retention requirements.

21. EMPLOYEE AND WORKPLACE PERSONAL INFORMATION

Employee personal information shall be processed only for lawful and legitimate employment, business and legal purposes.

This includes, where applicable: recruitment; identification; employment administration; payroll; benefits; performance management; disciplinary processes; training; health-related information; access control; CCTV; monitoring; termination; and legal and regulatory obligations.

Employees shall be informed about relevant processing through appropriate privacy notices and internal communications.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Access to employee information shall be limited to authorized persons with a legitimate business need.

22. CUSTOMER, RESELLER, SUPPLIER AND THIRD-PARTY PERSONAL INFORMATION

Tarsus processes personal information in connection with its distribution, customer onboarding, reseller management, credit, risk, compliance, sales, procurement and support activities.

Personal information may include information relating to: directors; beneficial owners; authorized representatives; shareholders; employees of customers or resellers; sole proprietors; suppliers; service providers; credit applicants; and other representatives.

Where applicable, processing may include: customer onboarding; KYC and verification; FICA-related processes; credit assessment; fraud prevention; sanctions screening; adverse media screening; risk assessment; account administration; collections; customer support; and contractual administration.

Tarsus shall ensure that such processing has an appropriate lawful basis and is conducted in accordance with applicable POPIA requirements.

23. TRAINING AND AWARENESS

Tarsus shall provide appropriate privacy and information protection awareness and training.

Training shall be proportionate to the employee's role and risk exposure.

At a minimum: employees shall receive privacy awareness training; relevant employees shall receive role-specific training; employees shall be made aware of breach reporting requirements; training completion shall be recorded; and refresher training shall be provided periodically.

24. MONITORING, COMPLIANCE AND ASSURANCE

Tarsus shall monitor compliance with this Policy using a risk-based approach.

Monitoring may include periodic compliance assessments; control testing; internal audits; third-party reviews; system reviews; privacy risk assessments; review of data subject requests; review of security incidents; training completion monitoring; Operator reviews; and remediation tracking.

Material findings shall be documented and assigned to responsible owners with appropriate remediation timelines.

25. MANAGEMENT REPORTING AND KEY PERFORMANCE INDICATORS

The Information Officer and/or designated responsible function shall provide appropriate privacy compliance reporting to management and relevant governance structures.

Reporting may include number of data subject requests; response times; number and severity of privacy incidents; personal information security compromises; training completion; Operator assessments; PIAs completed; overdue remediation actions; complaints; regulatory engagements; and material privacy risks.

26. NON-COMPLIANCE, EXCEPTIONS AND DISCIPLINARY ACTION

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Failure to comply with this Policy may expose Tarsus to legal, regulatory, financial, operational and reputational risk.

Employees who fail to comply may be subject to disciplinary action in accordance with applicable employment policies and procedures.

Third-party non-compliance may result in: corrective action; remediation requirements; contractual remedies; suspension of processing; termination of services; or other appropriate action.

Any exception to this Policy shall be documented; risk assessed; approved by an authorized person; time-bound where appropriate; and subject to compensating controls where required.

27. COMPLAINTS AND REGULATORY ENGAGEMENT

Data subjects may raise privacy-related concerns or complaints with Tarsus through the designated privacy contact.

Tarsus shall: acknowledge and record complaints; investigate appropriately; provide a response where required; maintain records; identify corrective actions; and escalate material matters to the Information Officer.

Where required, Tarsus shall cooperate with the Information Regulator and other competent authorities.

28. POLICY REVIEW

This Policy shall be reviewed at least annually and sooner where required due to changes in applicable law; regulatory developments; material changes to Tarsus's business; new processing activities; significant technology changes; material privacy incidents; audit findings; changes to governance structures; or other material developments.

The Policy Owner and Information Officer shall ensure that reviews are documented and that approved amendments are subject to formal document control.

29. RELATED POLICIES, STANDARDS AND PROCEDURES

This Policy shall be supported by, and read together with, applicable Tarsus policies, standards and procedures, including: Information Security Policy; Cybersecurity Policy; Data Classification and Handling Standard; Data Retention and Disposal Standard; Personal Information Security Compromise / Data Breach Response Procedure; Data Subject Request Procedure; Privacy Impact Assessment Procedure; Direct Marketing Procedure; Operator and Third-Party Privacy Standard; Cross-Border Data Transfer Procedure; Employee Privacy Notice; Customer/Reseller Privacy Notice; Supplier Privacy Notice; PAIA Manual; Records Management Policy; Acceptable Use Policy; Access Control Policy; and any applicable Group Compliance, Legal or Information Security policies.

30. CONTACT INFORMATION AND GOVERNANCE RESPONSIBILITIES

30.1 GOVERNANCE RESPONSIBILITIES

Role	Key Responsibilities
Information Officer	Executive accountability for POPIA compliance; provides strategic oversight; liaises with the Information Regulator; reports material privacy risks to Executive Management and the Board.

Docusign Envelope ID: C1B1B67F-6B53-8A67-8087-46BF235C4B09

Role	Key Responsibilities
Deputy Information Officer	Oversees implementation of the POPIA compliance programme; monitors compliance activities; reviews significant incidents and provides management oversight.
POPIA Administration Officer	Coordinates the day-to-day administration of the POPIA programme, including policy management, compliance monitoring, data subject requests, breach registers, privacy reporting, training coordination and record management.
Business Owners	Ensure personal information within their business processes is processed in accordance with this Policy.
Employees	Protect personal information, comply with this Policy, report incidents immediately and complete mandatory privacy awareness training.
Operators / Third Parties	Process personal information only in accordance with contractual obligations and applicable legislation and report any personal information security compromise to Tarsus without undue delay.

30.2 CONTACT INFORMATION

Contact	Details
Information Officer	*Head of Digital Transformation (to be confirmed)*
Deputy Information Officer	General Manager Legal Compliance, Risk, Debtors & HR- Compliance, Customer and Risk- Rene Du Plessis
POPIA Administration Officer	General Lead- Compliance, Customer and Risk - Pearl Masango
Data Subject Requests	*pmasango@tarsus.co.za or rduplessis@tarsus.co.za*
Personal Information Security Compromises	Incident reporting process *(to be confirmed)*