POPI Policy

Document Control

Document Number:	BF-HR-POL-025
Version Number:	1
Review Date:	
Next Review Date:	25/05/2027
Prepared by:	Elizma Els

Version History

Version	Date	Author	Approved by	Brief Description of Changes
1	25/05/2026	Elizma Els	CEO	First Version

1. Purpose of this policy

The purpose of this policy is to set mandatory rules and controls for the lawful, secure and accountable processing of personal information by the Company, particularly where the Company designs, builds, hosts, implements, integrates or supports software systems used by South African government clients.

This policy is designed to operationalise the Protection of Personal Information Act, 4 of 2013 (POPIA), the Promotion of Access to Information Act, 2 of 2000 (PAIA), the POPIA Regulations, official Information Regulator guidance, and related South African legal requirements that affect software, government systems, electronic records, cybersecurity, direct marketing and customer communications.

2. Legal and regulatory framework

Law / requirement	Application to this policy
POPIA	Main data protection law. Establishes lawful processing conditions, data subject rights, Information Officer duties, security safeguards, operator controls, breach notification, special personal information, children's information, direct marketing, automated decision-making and cross-border transfers.
POPIA Regulations, 2018	Prescribed forms and procedures, including objection, correction/deletion, direct marketing consent, complaints and prior authorisation processes.
PAIA	Access to records law. Requires PAIA manual, request-handling process and annual PAIA reporting where applicable.
Information Regulator guidance	Guidance on Information Officers/DIOs, special personal information, children's information, prior authorisation, direct marketing and PAIA annual reporting.
Cybercrimes Act, 19 of 2020	Relevant to cyber incidents, unauthorised access, malicious interference, evidence preservation and escalation.
Electronic Communications and Transactions Act, 25 of 2002	Relevant to electronic communications, electronic records, e-government services, electronic contracting, website notices and information system abuse.
Consumer Protection Act, 68 of 2008	Relevant to fair marketing, customer communications, direct marketing opt-outs, plain language and complaints where CPA applies.
Government contracts, SCM and procurement requirements	Government clients may impose stricter security, confidentiality, audit, data residency, breach notice and subcontractor requirements through contracts, SOWs, bid documents and security schedules.

3. Scope

This policy applies to all personal information processed by the Company in any format, including production databases, development/test environments, support

tickets, logs, backups, reports, exports, APIs, spreadsheets, screenshots, training materials, emails, messaging tools, project documentation, recordings and archives.

- citizen information processed in government applications, portals, mobile apps, case management tools, service-delivery systems or reporting platforms;
- government employee information processed through administrative, HR, workflow, access-control, support or identity-management functions;
- children's personal information, where a system or module captures or exposes information relating to persons under 18;
- special personal information, including health, biometric, criminal behaviour, race or ethnic origin, union membership, religious belief, political persuasion or similar high-sensitivity categories;
- Company employee, contractor, applicant, supplier, customer contact and user account information;
- metadata, logs and audit trails where those logs can identify a person or reveal user behaviour; and
- client-owned personal information processed by the Company as an operator under a government or other client contract.

4. POPIA principles adopted by the Company

Principle	Company rule
Accountability	The Company must be able to show who is responsible, what personal information is processed, why it is processed, where it is stored, who can access it and what controls protect it.
Processing limitation	Personal information may only be processed lawfully, fairly, minimally and for an authorised purpose.
Purpose specification	Every processing activity and product module must have a defined purpose and retention rule.
Further processing limitation	Personal information may not be reused for analytics, AI training, product improvement, benchmarking, demos, marketing or research unless compatible with the original purpose or separately authorised and lawful.
Information quality	Personal information must be kept accurate where the Company is responsible for maintaining it, and client correction requests must be supported where the Company acts as operator.
Openness	Appropriate privacy notices, PAIA manual, internal records and client data schedules must be maintained.
Security safeguards	Appropriate technical and organisational controls must protect confidentiality, integrity and availability.
Data subject participation	Data subjects must be able to exercise access, correction, deletion, objection and direct marketing opt-out rights through a controlled process.

5. Key definitions for this Company

Term	Meaning
Responsible party	The party that determines the purpose and means of processing. For government systems, this will usually be the government client for citizen or government employee data, unless a contract states otherwise.
Operator	A party that processes personal information for a responsible party under contract or mandate. The Company will usually be an operator for government client production data.
Data subject	The identifiable person to whom personal information relates, including citizens, children, government employees, Company employees, client users, suppliers and customer contacts.
Special personal information	High-sensitivity personal information, including health, biometric, criminal, race or ethnic origin, union, religious, political or similar categories under POPIA.
Child	A natural person under the age of 18. Children's information requires stricter controls and a documented lawful basis or authorisation.
Module	A specific product, platform, feature, database, workflow, report, API or app component that collects, stores, displays, transmits, exports or deletes personal information.

6. Roles and responsibilities

Role	Responsibility
Board / EXCO	Approve this policy, receive compliance reporting, ensure adequate resources and enforce accountability.
Information Officer	Own POPIA/PAIA accountability, maintain registrations, oversee this policy, approve high-risk processing and report to EXCO.
Deputy Information Officers	Manage delegated POPIA/PAIA duties in areas such as Legal, IT/Security, Product, Support, HR or Operations.
Legal / Compliance	Maintain PAIA manual, contracts, data processing schedules, lawful basis assessments, DSR/PAIA process and regulatory communications.
Product	Ensure privacy by design, module data registers, access models, export controls, retention capability and PIA gates.
Software Engineering	Implement secure SDLC, access controls, logging, API controls, data segregation, encryption and retention/deletion mechanisms.
Infrastructure / IT Security	Manage hosting, IAM, MFA, cloud regions, backups, monitoring, vulnerability management, incident response and access reviews.
Project Management / Implementation	Ensure data migration, go-live, client handover and training use approved data handling procedures.
Customer Support	Access client data only for support purposes, record ticket justification, mask sensitive data in tickets and escalate incidents.

HR	Maintain employee privacy notices, staff training, confidentiality undertakings and disciplinary enforcement.
Sales / Marketing	Use approved contracts, privacy notices, consent/opt-out controls and avoid unauthorised data use in campaigns.
All employees and contractors	Follow this policy, protect personal information, report incidents immediately and process only what is authorised.

7. Mandatory policy statements

- No product module, integration, report, export, API, data migration or support process may go live unless the relevant personal information has been identified, classified and recorded in the Product Module Data Register.
- Where the Company processes government client data, the Company must process only on documented client instruction and must not independently determine a new purpose for processing unless legally authorised and contractually approved.
- Production citizen, government employee or children's data may not be used for development, testing, training, demonstrations, analytics, AI model training or benchmarking unless it is anonymised or masked and formally approved through the privacy impact process.
- Children's personal information and special personal information must be treated as high risk by default and may only be processed where a documented lawful basis, client mandate and required safeguards exist.
- All access to production systems containing personal information must be named-user, role-based, least-privilege and logged. Shared accounts are prohibited unless formally approved as an exception with compensating controls.
- All exports and reports containing personal information must be restricted, logged and approved according to the data classification and client contract.
- All personal information breaches or suspected breaches must be reported immediately through the incident process, even where the facts are not yet confirmed.
- Where POPIA, a government contract or a security schedule sets a stricter requirement than this policy, the stricter requirement applies.

8. Processing rules

Rule	Mandatory standard
Lawful basis	Every processing activity must have a lawful basis, such as contract, legal obligation, consent, legitimate interest or documented client mandate. Consent must be recorded where used and withdrawal must be supported.
Purpose and minimality	Collect only the fields required for the authorised government or business purpose. Optional fields must be justified or removed.

Direct collection and notices	Where the Company collects directly from data subjects, a privacy notice must be provided at or before collection unless an exception applies.
Further processing and AI	Personal information may not be reused for AI, machine learning, analytics, product improvement, demo data, benchmarking or research unless approved through a PIA and legally/contractually permitted.
Accuracy	Data quality rules must be built into systems where the Company captures or maintains personal information. Correction workflows must exist where data subjects or government clients request corrections.
Retention	Retention must be linked to purpose, law and contract. Government client data must not be deleted or retained beyond instruction without documented legal/contract approval.
Deletion and destruction	Deletion must be secure, logged and capable of being evidenced. Backups must follow documented retention and restoration limits.

9. Government software system requirements

Because the Company designs and supports systems for South African government clients, each government contract or statement of work must include or be supported by a Data Processing and Security Schedule. At minimum, the schedule must record:

- the government client and the Company's roles as responsible party/operator for each dataset;
- the categories of data subjects, including citizens, government employees and children where applicable;
- the categories of personal information and special personal information;
- the authorised processing purposes and prohibited uses;
- hosting location, backups, logs, integrations and cross-border/sub-processor access;
- client data ownership, client instructions and client approval requirements;
- access roles, client admin roles, support access and audit logging expectations;
- incident and breach notification timelines, including client-specific SLA requirements;
- data return, deletion, retention and archival requirements at contract end; and
- audit rights, evidence requirements and subcontractor/sub-processor approval requirements.

10. Boxfusion implementation notes

For most government client production environments, Boxfusion acts primarily as an operator processing personal information on the documented instruction of the client as responsible party. Boxfusion may, however, act as responsible party for its own

internal processing activities, including employee, contractor, supplier, prospect, website and general business administration data, and may in limited cases act as responsible party for client-related processing where Boxfusion determines the purpose and means of processing under a separate lawful basis and contract position.

Boxfusion's government client handling model is contract-led and dataset-specific. For each government engagement, the applicable contract, statement of work, security schedule and delivery artefacts must identify the client owner, the relevant dataset, the role allocation between responsible party and operator, any data residency restrictions, approved support access, reporting/export rules, breach notification timelines and sub-processor limitations. Delivery, Product, Legal/Compliance and IT/Security must ensure that no module, implementation, migration, report, support activity or change is introduced outside the scope of the approved client instruction and contract position.

Boxfusion's incident escalation route requires any employee, contractor or supplier who becomes aware of a privacy, security or suspected personal information incident to escalate it immediately through the internal incident process to IT/Security, the operational owner and the Information Officer or delegated compliance lead. Where client data is affected, the relevant account, delivery or project owner must be engaged without delay so that contractual notification obligations can be assessed and actioned. High-risk incidents, confirmed breaches, regulatory exposure, cross-border risks or material client impact must be escalated to COO and EXCO level as required for containment, client communication, regulatory response and remediation oversight.

Boxfusion's privacy and security approval gates apply at minimum to new implementations, new modules, material change requests, integrations, data migrations, high-risk reports or exports, use of special personal information or children's information, changes to hosting architecture, onboarding of new sub-processors, and any proposed reuse of data outside the original approved purpose. The minimum gate requires review by the applicable business owner, Product, IT/Security and Legal/Compliance or Information Officer delegate, with formal sign-off before release, go-live or production access is granted where the risk level or contract requires it.

Boxfusion's hosting, cloud and sub-processor model must remain documented per client and environment. Hosting locations, backup locations, administrative access, SaaS tooling, managed service providers and any third-party sub-processors must be recorded and reviewed against client contract requirements, POPIA obligations and any South African data residency commitments. No new sub-processor, offshore support path or hosting change may be introduced for in-scope client data without the required internal review and, where contractually required, prior client approval.

Boxfusion's training and monitoring cadence must include POPIA, PAIA, confidentiality and information security awareness during onboarding, refresher training at least annually, and role-specific reinforcement for teams such as HR, Product, Engineering, Support, Delivery and Sales where they process or access personal information. Monitoring must include periodic access reviews, review of privileged activity and export logs, control checks on high-risk processes, incident trend review, and policy/register review at planned intervals so that compliance gaps are identified, escalated and tracked to closure.

10. Product Module Data Register

The Product Module Data Register is mandatory for every application, module, feature, report, integration, API or workflow that processes personal information. No high-risk module may proceed to go-live without an approved register entry and privacy/security sign-off.

Field	What must be captured
Module name and owner	Name, product owner, technical owner and support owner.
Client / environment	Government client, tenant, environment and whether the data is production, test, demo or training data.
Data subjects	Citizens, children, government employees, Company users, suppliers or other persons.
Data categories	Identity, contact, demographic, case/service data, health, education, financial, biometric, employment, location, logs, attachments and other fields.
Special / children flags	Whether the module includes children's information or special personal information, with lawful basis and controls.
Purpose and legal basis	Purpose of processing and whether based on client mandate, contract, law, consent or another basis.
Access roles	Client roles, Company roles, support roles, admin roles and privileged access.
Exports and reports	Allowed exports, approvers, fields, masking, frequency and logs.
Logs	Login, view, create, update, delete, export, admin and failed access logs.
Hosting and transfers	Cloud region, backups, sub-processors, support access and cross-border implications.
Retention and deletion	Retention period, archival, deletion/anonymisation method and client approval requirements.
Integrations and APIs	Interfaces, recipients, authentication, encryption, rate limits and data sharing basis.

11. Children's information and special personal information

Children's information and special personal information are high risk by default. Processing is prohibited unless a POPIA authorisation or exception applies, the

responsible party has a documented lawful basis, and the Company has approved technical and organisational safeguards.

- A Children's Information Register must be completed for any module that includes data relating to persons under 18.
- A Special Personal Information Register must be completed for health, biometric, criminal behaviour, race/ethnic origin, union membership, religious belief, political persuasion, sex life or similar high-risk data.
- Legal/Compliance must assess whether prior authorisation from the Information Regulator is required before the processing starts or materially changes.
- Children's information and special personal information must not be used in demos, training, development, testing, analytics or AI unless anonymised or unless a specific written approval is given after legal review.
- Access must be restricted to named roles, logged and reviewed monthly where risk is high.
- Reports and exports containing children's information or special personal information must require approval and must be logged.

12. Data subject rights and PAIA handling

The Company must maintain processes to support data subject rights under POPIA and access-to-records requests under PAIA. Where the request relates to government client data and the Company is an operator, the request must be routed to the government client unless the contract authorises the Company to respond directly.

Request type	Minimum process
Access request	Log request, verify identity/authority, identify whether Company or client data, respond or route to client, track deadline and outcome.
Correction/deletion request	Log request, verify identity/authority, assess legal/contract retention, correct/delete or assist client, record outcome.
Objection request	Log objection, assess lawful basis, restrict processing where required, update relevant systems.
Direct marketing opt-out	Apply opt-out immediately to suppression list and campaign tools; no further unsolicited electronic marketing to opted-out address/number.
PAIA request	Use PAIA process and manual; assess records, grounds for refusal, third-party notices, fees and response timelines.
Government client requests	Where client is responsible party, notify client immediately and support response within contract SLA.

13. Security compromise and incident response

A suspected or confirmed compromise of personal information must be reported immediately. A security compromise may include unauthorised access, loss, damage, deletion, theft, accidental disclosure, ransomware, misdirected email, exposed database, leaked export, unauthorised support access or third-party breach.

Step	Required action
1. Detect and report	Any employee, contractor or supplier must immediately report suspected incidents to IT/Security and the Information Officer using the incident channel.
2. Contain	IT/Security must preserve evidence, disable unauthorised access, isolate affected systems and prevent further disclosure or loss.
3. Assess	Legal/Compliance, IT and the business owner must assess personal information affected, data subjects, likely harm, client obligations and notification duties.
4. Notify	Where required, notify the Information Regulator and affected data subjects as soon as reasonably possible. Contractual client notice periods may be stricter and must be followed. Use the prescribed Regulator security compromise form/process where applicable.
5. Remediate	Fix root cause, reset credentials, patch systems, recover data, close exposed records and update controls.
6. Review	Prepare root cause analysis, lessons learned and control improvement actions for EXCO/Information Officer review.

14. Operators, sub-processors and cross-border transfers

- All suppliers that process personal information for the Company or government client systems must be listed in a Sub-Processor Register and assessed before onboarding.
- Supplier contracts must include confidentiality, security safeguards, breach notification, return/deletion, audit support, sub-processor restrictions and cross-border transfer provisions.
- The Company must maintain a Cross-Border Transfer Register covering hosting regions, backups, support locations, SaaS tools, sub-processors and international access to logs or data.
- Personal information may not be transferred outside South Africa unless the legal basis, contractual safeguards and client approval requirements have been assessed and recorded.
- Where a government contract requires South African data residency, no production data, backups, support access or logs may be transferred outside the approved location without written client approval.

15. Department-specific minimum controls

Department	Minimum controls
Sales / Bid Office	Use approved contract templates; ensure government data schedules; no unauthorised POPIA/security claims; maintain tender data pack; route privacy/security exceptions to Legal and IT.

Marketing / Communications	Use lawful consent or existing customer basis; maintain opt-out list; publish privacy/PAIA pages; do not use client/citizen data in marketing.
Business Analysis	Classify data in requirements; map data flows; avoid local copies; document access/export/reporting requirements.
Product	Maintain module data register; ensure privacy by design; approve access model, logs, exports, retention/deletion and high-risk processing before release.
Software Engineering	Implement secure SDLC, code review, API security, encryption, logging, tenant segregation and secrets management.
Testing / QA	Use synthetic or masked data; test access, exports, logs, deletion and tenant segregation; sanitise screenshots and defects.
Infrastructure / IT	Control cloud regions, MFA, IAM, privileged access, backups, monitoring, vulnerability management, endpoint security and DR.
Project Management / Implementation	Use client data handling plan; secure migration; approved go-live checklist; disable temporary accounts after go-live.
Training	Use demo data only; do not expose real citizen/children/special data; keep training attendance and materials.
HR	Protect employee/applicant data; issue employee privacy notice; manage confidentiality, training, onboarding/offboarding and access removal.
Finance	Protect banking, payroll, billing and supplier data; apply access controls and retention.
Customer Support	Access client data only against a ticket; mask attachments; restrict exports; escalate incidents and DSR/PAIA requests.

16. Annexure A: Control measures checklist

The following controls are mandatory unless formally marked as not applicable by the Information Officer after documented assessment. Evidence must be available for every control marked as implemented.

Governance and accountability

ID	Control measure	Evidence required	Owner	Review
GOV-01	Register the Information Officer with the Information Regulator.	Regulator registration confirmation and portal screenshot.	Information Officer / Legal	Annual / on change
GOV-02	Appoint and register Deputy Information Officers for Legal,	Appointment letters, delegation	COO / Legal	Annual / on change

	IT/Security, Product/Support and HR where needed.	matrix and registration proof.		
GOV-03	Maintain a POPIA processing register covering all Company and client processing activities.	Processing register with owner sign-off.	Compliance / Operations	Quarterly
GOV-04	Maintain responsible party/operator role mapping for each government contract and dataset.	Client data role matrix and contract schedule.	Legal / Sales / Delivery	Per contract
GOV-05	Require privacy/security impact assessment for new modules, integrations, reports, exports and high-risk changes.	Approved PIA/DPIA checklist.	Product / Legal / Security	Per project/release
GOV-06	Report POPIA/PAIA compliance status, incidents and high-risk gaps to EXCO.	EXCO pack, minutes and action tracker.	Information Officer / COO	Monthly/quarterly

Contracts and government client controls

ID	Control measure	Evidence required	Owner	Review
CON-01	Include data processing and security schedule in each government client contract/SOW.	Signed schedule or contract annexure.	Legal / Sales	Per contract
CON-02	State client data ownership and prohibit Company reuse except as expressly authorised.	Contract clause and approved purpose list.	Legal	Per contract
CON-03	Maintain approved sub-processor list and obtain client approval where	Sub-processor register and approvals.	Legal / Procurement / IT	Quarterly

	contract requires.			
CON-04	Bind employees, contractors and suppliers to confidentiality obligations.	Employment/contractor/vendor confidentiality clauses.	HR / Legal / Procurement	Onboarding / annual
CON-05	Define client audit rights and evidence package for government due diligence.	Audit evidence index and contract clauses.	Legal / Operations	Per contract / audit
CON-06	Define return, deletion, archival and destruction obligations at contract end.	Exit plan, deletion certificate template and retention schedule.	Legal / Delivery / IT	Per contract/end of service

Data collection and lawful processing

ID	Control measure	Evidence required	Owner	Review
DAT-01	Document purpose and minimum necessary fields for each module/process.	Module data register and field list.	Product / Business Analysis	Per release
DAT-02	Document lawful basis or client mandate for each data category.	Lawful basis matrix / contract instruction.	Legal / Product	Per module/process
DAT-03	Publish and maintain applicable privacy notices for Company-collected data.	Website/HR/client notices and screenshots.	Legal / Marketing / HR	Annual / on change
DAT-04	Implement accuracy and correction workflows where data is maintained by the Company.	Correction process and test evidence.	Product / Support	Quarterly
DAT-05	Prohibit further processing for analytics, AI, demos, product improvement or research unless approved.	Further-processing approval register.	Legal / Product / Data	Per use case

DAT-06	Apply retention/deletion rules per data category and client contract.	Retention schedule and deletion logs.	Operations / IT	Monthly/annual

Product and module controls

ID	Control measure	Evidence required	Owner	Review
MOD-01	Complete Product Module Data Register before go-live.	Completed register entry.	Product Owner	Per module/release
MOD-02	Maintain RBAC matrix per module and role.	Access matrix and system role configuration.	Product / Engineering	Per release / quarterly
MOD-03	Enforce tenant/client data segregation.	Architecture diagram and tenant segregation test results.	Engineering / Architecture	Per release / annual
MOD-04	Restrict exports and reports to approved roles.	Export permission matrix and log sample.	Product / Engineering	Monthly review
MOD-05	Require approval for bulk downloads or high-risk exports.	Approval workflow and export logs.	Product / Support / Client Admin	Per export
MOD-06	Mask high-risk fields where full visibility is not required.	Masking rules and screenshots.	Product / Engineering	Per release
MOD-07	Log view, create, update, delete and export events for high-risk modules.	Audit log sample.	Engineering / IT	Continuous / monthly review
MOD-08	Log all administrator and privileged actions.	Admin audit log report.	IT / Engineering	Monthly
MOD-09	Secure APIs with authentication, authorisation, rate limits and logging.	API standard, gateway config and tests.	Engineering	Per release
MOD-10	Control data migration using secure transfer, validation and deletion of staging files.	Migration plan, transfer log and deletion proof.	Implementation / Engineering	Per migration

Children and special personal information

ID	Control measure	Evidence required	Owner	Review
SPC-01	Maintain Special Personal Information Register.	Register and legal basis memo.	Legal / Product / HR	Quarterly
SPC-02	Maintain Children's Information Register where children's data is processed.	Children's data register and safeguards.	Legal / Product	Quarterly
SPC-03	Confirm competent person consent or statutory/client authorisation for children's data.	Consent/authorisation evidence or client legal instruction.	Legal / Client Owner	Per module/process
SPC-04	Assess prior authorisation requirement before high-risk processing starts.	Prior authorisation assessment / application evidence.	Legal / Information Officer	Per high-risk activity
SPC-05	Restrict children/special data access to named roles and log access.	Role matrix and access logs.	IT / Product	Monthly
SPC-06	Prohibit profiling/direct marketing involving children unless legally approved.	Marketing exclusion list and approval register.	Marketing / Legal	Per campaign/use case

Security safeguards

ID	Control measure	Evidence required	Owner	Review
SEC-01	Apply MFA to privileged, remote and high-risk access.	MFA report.	IT	Monthly
SEC-02	Use least-privilege access and JML access changes.	Access requests, leaver reports and review sign-off.	IT / HR	Monthly/quarterly
SEC-03	Encrypt personal information in transit and at rest where technically feasible and appropriate.	TLS certificates, DB/storage encryption settings.	IT / Engineering	Quarterly

SEC-04	Use secrets management; no credentials in code or tickets.	Vault logs and secrets scan report.	Engineering / IT	Monthly/per release
SEC-05	Back up critical data and test restore capability.	Backup logs and restore test report.	IT	Daily backups / quarterly restore test
SEC-06	Perform vulnerability scanning, dependency scanning and patch management.	Scan reports and remediation tracker.	IT / Engineering	Monthly/per release
SEC-07	Review cloud/network security configurations.	Cloud security posture report and firewall/security group review.	Infrastructure	Quarterly
SEC-08	Monitor security logs and alerts for high-risk systems.	SIEM/monitoring report and incident tickets.	IT Security	Continuous / monthly review
SEC-09	Protect endpoints with encryption, EDR/AV, patching and remote wipe where applicable.	Endpoint compliance dashboard.	IT	Monthly

Software development and testing

ID	Control measure	Evidence required	Owner	Review
DEV-01	Operate secure SDLC with security requirements and release gates.	Secure SDLC policy and release checklist.	Engineering / Product	Per release
DEV-02	Include privacy impact gate in SDLC for new personal information processing.	PIA approval in project/release file.	Product / Legal	Per release
DEV-03	Require peer code review before merge/deployment.	Pull request approval history.	Engineering	Every change
DEV-04	Perform security and privacy test cases before release.	Test cases and pass/fail evidence.	QA / Engineering	Per release
DEV-05	Use synthetic or masked data in dev/test; prohibit raw production personal data unless exception approved.	Test data policy and masking evidence.	QA / Engineering	Per test cycle

DEV-06	Control production access through approved support/break-glass process.	Access approval and session logs.	IT / Support / Engineering	Per access/monthly review
DEV-07	Scan open-source and third-party dependencies for vulnerabilities and licence risks.	SCA report and remediation evidence.	Engineering	Per release/monthly

Support, implementation and training

ID	Control measure	Evidence required	Owner	Review
OPS-01	Allow support access only for a valid ticket or approved support purpose.	Ticket-linked access logs.	Support / IT	Monthly
OPS-02	Mask personal information in screenshots, logs and attachments where possible.	Sanitised ticket samples and SOP.	Support / QA	Monthly sample
OPS-03	Use secure data transfer and migration procedures.	Migration checklist and transfer logs.	Implementation	Per migration
OPS-04	Disable temporary implementation accounts after go-live.	Go-live checklist and access report.	Implementation / IT	Per go-live
OPS-05	Use demo or synthetic data for training and demonstrations.	Demo environment proof and training material samples.	Training / Product	Per training/demo
OPS-06	Train employees and contractors on POPIA, PAIA, security and role-specific data handling.	Training attendance and assessment results.	HR / Compliance	Onboarding/annual

Data subject rights and PAIA

ID	Control measure	Evidence required	Owner	Review

DSR-01	Maintain data subject request workflow for access, objection, correction and deletion.	DSR SOP and request register.	Legal / Support	Per request/monthly
DSR-02	Implement correction/deletion support in relevant modules or documented manual process.	Feature test evidence or manual SOP.	Product / Support	Per module/quarterly
DSR-03	Maintain and publish PAIA Manual.	PAIA manual URL and version log.	Legal	Annual/on change
DSR-04	Maintain PAIA request register and response templates.	PAIA register and sample response file.	Legal	Per request
DSR-05	Submit annual PAIA report where applicable.	Information Regulator submission confirmation.	Information Officer / Legal	Annually by 30 June
DSR-06	Route government client data requests to the client responsible party unless authorised to respond.	Request routing log and client notification.	Legal / Support	Per request

Incidents and breach notification

ID	Control measure	Evidence required	Owner	Review
INC-01	Maintain security compromise response plan.	Incident response plan and call tree.	IT / Legal / COO	Annual test
INC-02	Use Information Regulator security compromise notification process/form where required.	Completed SCN1 or portal submission evidence.	Information Officer / Legal	Per breach
INC-03	Meet client-specific breach notification SLA.	Contract SLA tracker and notification evidence.	Legal / Account Owner	Per incident
INC-04	Preserve evidence for cyber/privacy incidents.	Evidence log, logs retained, chain of custody.	IT Security / Legal	Per incident
INC-05	Perform root-cause analysis and control improvement after incidents.	RCA report and action tracker.	IT / COO	Per incident

Cross-border and third-party processing

ID	Control measure	Evidence required	Owner	Review
XBD-01	Maintain cloud/data residency register.	Cloud region and backup location evidence.	IT / Legal	Quarterly
XBD-02	Assess legal safeguards before any cross-border transfer or offshore support access.	Cross-border assessment memo.	Legal / IT	Per transfer/change
XBD-03	Review offshore sub-processor and support access.	Sub-processor DPA and access scope.	Procurement / Legal / IT	Annual/per supplier
XBD-04	Enforce data residency commitments in government contracts.	Hosting evidence and contract mapping.	IT / Legal	Quarterly/per contract

Marketing, electronic communications and customer communications

ID	Control measure	Evidence required	Owner	Review
MKT-01	Record consent or lawful basis for electronic direct marketing and provide opt-out.	Consent logs and campaign sample.	Marketing	Per campaign/monthly
MKT-02	Publish website privacy, PAIA and cookie/tracking notices.	Live URL and cookie scan.	Marketing / Legal	Quarterly
MKT-03	Use approved electronic contracting terms and records.	Signed e-contract audit trail.	Sales / Legal	Per contract
MKT-04	Operate complaints and unsubscribe handling process.	Complaint/opt-out register.	Support / Marketing	Monthly

Monitoring and assurance

ID	Control measure	Evidence required	Owner	Review
MON-01	Review user access to critical and high-risk systems.	Access review sign-off.	IT / Data Owners	Monthly/quarterly
MON-02	Review audit logs for privileged actions, exports and unusual access.	Log review report.	IT Security / Compliance	Monthly

MON-03	Test key POPIA controls and record pass/fail outcome.	Control testing worksheet.	Compliance / Internal Audit	Quarterly
MON-04	Review operators and sub-processors for compliance evidence.	Vendor review checklist.	Procurement / Legal / IT	Annual
MON-05	Review this policy, PAIA manual, registers and training annually.	Policy review record and approvals.	Information Officer / Legal	Annual

17. Boxfusion register implementation notes

Boxfusion must maintain the following registers as controlled operational records to evidence POPIA and PAIA compliance and to support internal governance, client assurance and audit readiness: the Personal Information Processing Register, Product Module Data Register, Children's Information Register where applicable, Special Personal Information Register where applicable, Cross-Border Transfer Register, Sub-Processor Register, Data Subject Request Register, Security Compromise or Breach Register, Access Review Register, Training Register, applicable PAIA request and annual reporting records, and any supporting retention, exception or test-data registers required by this policy. Each register must have a named owner, a defined update trigger, a review cadence, evidence of review, and a clear escalation route where gaps, overdue actions or high-risk exposures are identified. Where a register applies only to certain products, clients, departments or processing scenarios, the responsible owner must explicitly confirm applicability or non-applicability and ensure that the supporting evidence is retained.

17. Annexure B: Minimum documents, forms and registers

Document / register	Minimum purpose
Information Officer and DIO registration proof	Proof of regulator registration and delegated POPIA/PAIA responsibilities.
PAIA Manual	Published record-access manual with contact details, request process and records categories.
PAIA request register and annual reporting evidence	Track PAIA requests and annual submission to the Information Regulator.
Personal Information Processing Register	Central record of processing activities, systems, purposes, legal basis, retention and sharing.
Product Module Data Register	Module-level data types, access, exports, logs, hosting, retention and risk flags.
Children's Information Register	Modules/processes containing children's data and lawful basis/safeguards.
Special Personal Information Register	Special data categories, access, lawful basis and prior authorisation assessment.

Cross-Border Transfer Register	Cloud regions, offshore access, sub-processors and legal safeguards.
Sub-Processor Register	Third parties processing personal information and approved contracts/security status.
Data Processing Agreement / Operator Schedule	Contractual POPIA section 21 and government-client security obligations.
Data Subject Request Register	Access, objection, correction, deletion and opt-out requests with outcomes.
Security Compromise / Breach Register	Incident details, containment, notifications and root-cause actions.
Data Retention Schedule	Retention and deletion rules by record type and client contract.
Secure SDLC checklist	Privacy/security gates for requirements, design, development, testing and release.
Test Data Exception Register	Approved exceptions where production data is used outside production.
Access Review Register	Periodic review of user/admin/support access.
Training Register	Employee and contractor completion of POPIA, PAIA and security training.

18. Policy breaches and enforcement

Failure to comply with this policy may result in disciplinary action, contract termination, removal of system access, supplier remediation, legal action or reporting to regulators or clients, depending on the severity of the breach. Any deliberate unauthorised access, concealment of a breach, unauthorised export or misuse of citizen, children's or government employee information will be treated as a serious breach.

19. Exceptions

Exceptions to this policy may only be approved in writing by the Information Officer, after Legal and IT/Security assessment. Exceptions must be time-bound, risk-assessed, recorded in an exceptions register and supported by compensating controls.

20. References used for this draft

Source	Use in policy
Protection of Personal Information Act 4 of 2013	South African Government / Department of Justice official Act.
Regulations relating to the Protection of Personal Information, 2018	Government Gazette regulations under POPIA.
Information Regulator Guidance Note on Information	Guidance on registration and duties of IOs/DIOs.

Officers and Deputy Information Officers	
Information Regulator POPIA Forms	Objection, correction/deletion, direct marketing consent, complaints, security compromise notification and prior authorisation forms.
Information Regulator guidance on children's information, special personal information and prior authorisation	Guidance relevant to children and special personal information.
Information Regulator PAIA Annual Report guidance and eServices	Annual PAIA reporting process and due dates.
Electronic Communications and Transactions Act 25 of 2002	Electronic communications, transactions, e-government services and information-system abuse context.
Cybercrimes Act 19 of 2020	Cyber incidents, unauthorised access and malicious interference context.
Consumer Protection Act 68 of 2008	Direct marketing, fair customer communications and complaints context where applicable.

21. Approval

Role	Name	Signature	Date
Information Officer			
COO			
IT / Security			
EXCO / Board representative			