

**BROKSTOCK SA (PTY) LTD**  
**Anti-Money Laundering, Terrorist and**  
**Proliferation Financing Policy (FIC or AML Policy)**

Last updated: November  
2025

Next review: November  
2026

**Contents**

1. INTRODUCTION.....	3
2. WHAT ARE SANCTIONS? .....	4
3. REGULATORY FRAMEWORK.....	4
4. ANTI-MONEY LAUNDERING (AML) STATEMENT .....	4
5. SANCTIONS .....	5
6. RESPONSIBILITY FOR THE POLICY.....	5
7. RISK ASSESSMENT .....	6
8. OUR RISK PROCEDURES .....	6
9. REPORTING CONCERNS .....	9
10. RECORD KEEPING .....	9
11. TRAINING .....	10
12. CONSEQUENCES OF NON-COMPLIANCE .....	10
13. AMENDMENTS TO THIS POLICY .....	10
14. POLICY REVIEW .....	11
15. OWNERSHIP OF THIS POLICY .....	11
ANNEXURE 1: SANCTIONS REPORT FORM (internal – to be submitted to the Company’s Authorised Person) .....	12
ANNEXURE 2: SANCTIONS REPORT FORM (external – to be submitted to the Financial Intelligence Centre) .....	16

## 1. INTRODUCTION

- 1.1.** BROKSTOCK SA (PTY) LTD (hereinafter "BROKSTOCK", the "Company" or "We") is incorporated under the laws of South Africa and is registered with the Companies and Intellectual Property Commission under registration number 2020/523823/07. BROKSTOCK is a brand operated by BROKSTOCK SA (PTY) LTD, a company incorporated and registered under South African law and an investment firm regulated by the Financial Sector Conduct Authority ("FSCA") with license number 51404. This Policy is recommended for employees of financial institutions by various bodies, including the Financial Sector Conduct Authority (FSCA) and the South African Reserve Bank (SARB).
- 1.2.** This Policy ("the Policy") is issued by BROKSTOCK SA (PTY) LTD (the "Company") and applicable to the directors and employees of the Company, as well as contractors (the "Responsible Persons") for the purpose of complying with applicable sanctions laws.

## DEFINITIONS

**"Accountable Institution"** means a business that falls within the scope of Schedule 1 to the Financial Intelligence Centre Act ("FIC Act") that is required to implement customer due diligence, recordkeeping, reporting and risk management measures.

**"Authorised Representative"** means any natural person who acts on behalf of a legal entity client, whether formally appointed through a resolution, mandate, power of attorney, or by virtue of office. Screening applies to both the entity and its authorised representatives.

**"Beneficial Owner"/"Ultimate Beneficial Owner (UBO)"** means a natural person who ultimately owns or exercises effective control over a legal entity or legal arrangement, directly or indirectly, through ownership, voting rights, influence, or other means.

**"Client"** means any natural person or legal entity with whom the Company establishes or proposes to establish a business relationship or executes a transaction.

**"Customer Due Diligence (CDD)"** means the process of identifying and verifying a client's identity, including verification of beneficial ownership, the nature of the relationship, and ongoing monitoring.

**"Enhanced Due Diligence (EDD)"** means additional measures applied to High Risk clients, which may include obtaining source of funds, source of wealth, additional documentation, adverse media reviews, independent verification, and senior management approval.

**"Legal Entity"** means any juristic person recognised under South African or foreign law, including companies, close corporations, non-profits, partnerships with juristic

personality, and equivalent foreign entities.

**“Politically Exposed Person (PEP)”** means an individual entrusted with prominent public functions, as well as their immediate family members and close associates. PEPs include foreign PEPs, domestic PEPs, and individuals associated with international organisations.

**“Sanctions Screening”** means the process of assessing whether a client or related party appears on sanctions lists issued by the United Nations, the South African government, foreign regulators, or other competent authorities. Sanctions prohibit the establishment or continuation of a business relationship.

## 2. WHAT ARE SANCTIONS?

- 2.1.** Sanctions are restrictions on activities with targeted countries, governments, entities, individuals and industries (“the Targets”) that are imposed by bodies such as the United Nations (UN), individual countries or groups of countries such as the European Union (EU).

## 3. REGULATORY FRAMEWORK

- 3.1.** South Africa’s targeted financial sanctions regimes originate from resolutions of the United Nations Security Council (“UNSC”) under Chapter VII of the Charter of the United Nations. South Africa implements two distinct targeted financial sanctions regimes through the Financial Intelligence Centre Act, 2001 and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004, which form part of the regulatory framework relating to anti-money laundering (“AML”) and countering the financing of terrorism.
- 3.2.** The Financial Action Task Force (“FATF”) Recommendations 6 and 7 also require the implementation of the UNSC Resolutions on the targeted financial sanctions regime for all FATF member countries.
- 3.3.** It is also necessary to maintain the sanctions of the EU, United Kingdom (“UK”), United States of America (“USA”) and other countries against terrorist entities, especially against Al Qaeda, the Taliban, the Islamic State of Iraq and the Levant, amongst others.
- 3.4.** Target in this context refers to any activity, country or person that relates to organised crime, illegal drugs, human trafficking, corruption, and terrorism.

## 4. ANTI-MONEY LAUNDERING (AML) STATEMENT

- 4.1.** The Company may not:

- 4.1.1.** deal with funds or economic resources owned, held or controlled by a Target where the Company knows or has reasonable grounds to suspect that a Target is

holding or controlling those funds or economic resources;

**4.1.2.** make funds, financial services or economic resources available, directly or indirectly, to Targets;

**4.1.3.** make funds, financial services or economic resources available, directly or indirectly, for the benefit of Targets; and

**4.1.4.** knowingly and intentionally participate in activities that would directly or indirectly circumvent the financial restrictions imposed by the sanctions regime or enable or facilitate the commission of any of the above.

**4.2.** The Financial Intelligence Centre (“FIC”) is the principal body that assists in the implementation of financial sanctions pursuant to resolutions adopted by the Security Council of the UN, under Chapter VII of the Charter of the United Nations.

## **5. SANCTIONS**

**5.1.** The sanctions regime is not the same as the AML regime.

**5.2.** There is no distinction in the sanctions regime between regulated and non-regulated sectors or activities. The sanctions regime applies to all services and products offered by the Company.

**5.3.** A sanctions regime prevents the use of all financial resources by or for the benefit of Targets: it is irrelevant that the funds and purpose of the transaction are legal. Conversely, the AML regime is aimed at disrupting the flow of criminal property, i.e. property that constitutes or represents a person's benefit from criminal conduct.

**5.4.** In the case of legal entity clients, sanctions controls apply both to the entity and to any individuals who own or control it or act on its behalf.

## **6. RESPONSIBILITY FOR THE POLICY**

**6.1.** The person who has overall responsibility for this Policy is the Director(s) of the Company (“Authorised Person”).

**6.2.** The Authorised Person is responsible for ensuring this Policy is adhered to by all staff and is responsible for maintaining a register of all reports they receive under this Policy.

**6.3.** Financial sanctions relating to a specific country or terrorist group are sanctions regimes. They have specific regulations, and various forms of conduct are prohibited depending on the particular regulations. Regulations are imposed by the UN Security Council, and it is important to regularly review and assess which countries are currently under sanctions.

The updated sanctions lists can be accessed from:

UN sanctions - [https://www.un.org/securitycouncil/sanctions/1267/aq\\_sanctions\\_list](https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list);

EU sanctions - <https://www.sanctionsmap.eu/#/main>;

UK sanctions - <https://www.gov.uk/government/publications/the-uk-sanctionslist>;

UK Office of Financial Sanctions Implementation -

<https://www.gov.uk/government/collections/financial-sanctions-regime-specificconsolidated-lists-and-releases>; and

Office of Foreign Assets Control sanctions - <https://sanctionssearch.ofac.treas.gov/>

## **7. RISK ASSESSMENT**

**7.1.** The Company aims to ensure that this Policy and its procedures are proportionate to the risks faced.

**7.2.** This Policy and the procedures contained below have been developed in response to the results of that risk assessment. Where necessary, risk assessment shall be reviewed, and appropriate changes to this Policy shall be made and this Policy amended from time to time.

## **8. OUR RISK PROCEDURES**

**8.1.** Screening Clients:

**8.1.1.** Before entering into a relationship with a client, the Company conducts a thorough screening of all applicants against blacklists, PEP lists, sanctions lists, and other relevant databases. The Company also implements ongoing monitoring, which involves continuous automated screening of existing clients against blacklists and other applicable watchlists.

**8.2.** The Company conducts screenings before:

**8.2.1.** providing any services to an individual, entity, or other type of legal person; and

**8.2.2.** receiving or transferring funds to, from or on behalf of an individual entity, or other type of legal person.

**8.2.3.** The Company ensures that the screening process is designed to mitigate risks related to money laundering, terrorist financing, and other unlawful activities.

**8.2.4.** The screening and monitoring processes comply with applicable regulatory requirements and international best practices, ensuring adherence to the highest compliance standards.

**8.2.5.** The Company uses advanced technological solutions for automated monitoring and screening, enabling real-time checks and timely identification of potential risks.

### **8.3. Screening Others**

**8.3.1.** The Company may onboard both natural persons and legal entities. Where the applicant is a legal entity, screening extends to the entity itself, its directors, beneficial owners, and any authorised representatives.

**8.3.2.** In addition to screening clients, we follow the above screening procedures for intended recipients of funds in transactional and litigation matters, where we have reason to believe that they may be subject to sanctions.

### **8.4. Screening Match Process**

**8.4.1.** Any potential match identified through the Company's screening process shall be properly investigated by the Key Individual before taking any further steps with client engagement or otherwise.

**8.4.2.** Responsible Persons shall immediately report any potential matches to the Authorised Person.

**8.4.3.** The Authorised Person must then investigate whether there is an actual match.

**8.4.4.** The result of such an investigation may be that the Company:

- seeks guidance from the FIC; and/or
- requests an external party to investigate whether the person or entity the Company is dealing with is, in fact, a Target.

**8.4.5.** Where there is a positive match against the sanctions lists, the Company's obligations include the following:

- reporting the case to the FIC;
- freezing property and transactions; and
- not dealing with or engaging with the person or entity in question.

**8.4.6.** It is not for Responsible Persons to decide whether there is a positive match and if so, whether the Company should act. The Responsible Person's responsibility is simply to complete the AML Report Form and submit it to the Authorised Person, who is responsible for deciding how to proceed.

**8.4.7.** Automatic AML system SumSub will be used to identify an applicant's presence on or absence from global or local sanctions lists, PEP lists, watchlists, blocklists, or adverse media sources. The responsible employee will check the results of the check performed. Additionally, all clients must be asked whether they fall into this category.

### **8.5. Risk-Based Approach**

We utilise a Risk-Based Approach to classify clients into Standard and High Risk categories based on various factors, including:

- The nature of the client's business activities;
- Geographical location of the client;
- Transaction patterns and behaviours.

This classification determines the level of Customer Due Diligence (CDD) and monitoring applied.

For legal entity clients, the risk classification reflects the nature of the entity's ownership and control structure, jurisdiction, and transparency of information.

Entities with foreign incorporation, multi-layered or opaque ownership, nominee arrangements, offshore elements, or any PEP exposure are treated as High Risk and are subject to enhanced scrutiny in accordance with the Company's RMCP and Onboarding Manual.

### **8.6. Periodic Reviews**

The Company conducts Periodic Reviews of all client relationships to ensure that:

- The risk classification of clients remains accurate.
- Client information is updated.
- Any unusual or suspicious activity is identified promptly.

The frequency of these reviews depends on the client's assigned risk level.

- Standard Risk: Reviews are conducted at least annually.
- High Risk: Reviews are conducted more frequently, as determined by the risk assessment.

Legal entity clients are monitored on the same basis as natural persons, with risk-based adjustments where ownership structures, jurisdictions, or business activities warrant increased vigilance. Any material changes in ownership or control must trigger a reassessment of the client's risk classification.

There is also ongoing due diligence in place, by which the Company keeps clients' information up-to-date. We conduct a thorough review of all clients on an annual basis and carry out unplanned checks in risky situations (blacklisting, failure to provide required documents, etc.).

### **8.7. Regular Name Screening**

The Company conducts regular name screening against:

- Sanctions lists.

- Politically Exposed Persons (PEP) databases.
- Adverse media and other relevant watchlists.

This screening occurs at onboarding and regularly throughout the client relationship to identify any changes in risk.

Ongoing screening is carried out to ensure the alignment of available client information with the most up-to-date and accurate data. This process helps identify and prevent any discrepancies that may arise due to outdated or incorrect records. It also includes monitoring for any changes in client status, such as their inclusion in any of the specified lists or other compliance-related updates. By maintaining this proactive approach, we aim to uphold the highest standards of accuracy and regulatory compliance.

### **8.8. Transaction Monitoring**

The Company will conduct transaction monitoring as part of this AML Policy. This approach will enable the proactive detection and reporting of unusual or suspicious transactions, ensuring compliance with the Financial Intelligence Centre Act (FICA).

## **9. REPORTING CONCERNS**

**9.1.** Where a Responsible Person is concerned that:

**9.1.1.** a matter involves a Target; or

**9.1.2.** an offence has been committed under an AML or Sanctions Regime, such Responsible Person must raise the concern with the Authorised Person.

**9.2.** If a Responsible Person believes a sanctions issue and possible money laundering or terrorist financing issue are involved, this must be reported to the Authorised Person immediately.

## **10. RECORD KEEPING**

**10.1.** For a Business Relationship, records must be kept for at least 5 years from the date on which the Business Relationship is terminated.

**10.2.** For transactions, the records in respect of the Single Transaction or any other transaction must be kept for at least 5 years from the date on which the transaction is concluded.

**10.3.** Suspicious Transaction Reporting: If a transaction is reported to the FIC under section 29 of FICA, then the records must be kept for at least 5 years from the date on which the report is made.

**10.4.** The need to maintain adequate records for at least 5 years gives effect to the

provisions of FICA and is essential to assist with the ultimate investigation and prosecution of crime, if applicable.

## **11. TRAINING**

- 11.1.** All Company employees will receive AML training from time to time, and it is compulsory.
- 11.2.** New employees will receive training as part of the induction process. Further AML training will be provided to Company employees at least every two years or whenever there is a substantial change in the law or the Company's Policy and procedure.
- 11.3.** AML training will cover:
- 11.3.1.** the law relating to the AML regime; and
  - 11.3.2.** this Policy and procedures.
- 11.4.** The Authorised Person will continually monitor training needs, but if the Responsible Person feels that such Responsible Person needs further training on any aspect of the relevant law or our Sanctions Policy or procedures, the Authorised Person shall be contacted.

## **12. CONSEQUENCES OF NON-COMPLIANCE**

- 12.1.** Failure to comply with this Policy puts both the relevant Responsible Person and the Company at risk.
- 12.2.** The Company takes compliance with this Policy very seriously, and failure to comply with any requirement of it may, therefore, lead to disciplinary action being taken by the Company under the relevant Company procedures. This may, in turn, result in disciplinary action being taken against an employee, including possible dismissal in accordance with local Labour Law.
- 12.3.** The details of the Company's Authorised Person in relation to this Policy are as follows:

Authorised Person: Petrus Johannes Serfontein  
Number: 080 022 7672, +27 12 001 9206  
E-mail: pserfontein@brokstock.co.za

## **13. AMENDMENTS TO THIS POLICY**

- 13.1.** Amendments to this Policy will take place from time to time, subject to BROKSTOCK's discretion and pursuant to any changes in the law. Such changes will be brought to the

attention of employees, members and clients where they are affected.

## **14. POLICY REVIEW**

- 14.1.** The Key Individual has the authority to make amendments to this Policy. The Key Individual may delegate responsibility to an employee or external party to draft the amendments.
- 14.2.** If any inadequacy of any element of this Policy is identified, that portion of the Policy can be amended. The Policy should also undergo a full review as deemed necessary.
- 14.3.** The Policy shall be reviewed at least annually, and more frequently.
- 14.4.** Any significant changes in the Policy after each review shall follow a formal approval process.

## **15. OWNERSHIP OF THIS POLICY**

- 15.1.** This Policy is owned by BROKSTOCK SA (PTY) LTD, trading as BROKSTOCK, an authorised financial services provider in terms of the Financial Advisory & Intermediary Services Act (37 of 2002) and subordinate legislation, with FSP number 51404.
- 15.2.** The Key Individual of BROKSTOCK SA (PTY) LTD hereby confirms the adoption of this Policy on behalf of the governing body of BROKSTOCK SA (PTY) LTD and accepts responsibility for the successful training of employees and implementation of this Policy.

This Policy is hereby approved and signed by:

---

Petrus Johannes Serfontein, the Key Individual

BROKSTOCK SA (PTY) LTD

## ANNEXURE 1: SANCTIONS REPORT FORM (internal – to be submitted to the Company’s Authorised Person)

1. This form should be used in accordance with this Policy in reporting all relevant information to the Authorised Person, including information regarding suspected designated persons and suspected breaches of financial sanctions.
2. The Company’s and its employees’ AML reporting and compliance obligations are described in BROKSTOCK SA (PTY) LTD’s Anti-Money Laundering, Terrorist and Proliferation Financing Policy (FIC or AML Policy). Please review this Policy carefully prior to completing this form.
3. Following completion, please e-mail the completed form, including any associated documents, to [pserfontein@brokstock.co.za](mailto:pserfontein@brokstock.co.za) or [compliance@brokstock.co.za](mailto:compliance@brokstock.co.za).

1.	Details of the person completing this report			
	Name (including title)			
	Job title			
	Company/organisation			
	Address			
	Contact number(s)			
	Email address			
	Date submitted (dd/mm/yyyy)			
2.	Are you submitting this form on behalf of a third party?	Y		N
3.	What are you reporting?			
	Suspected designated person		Suspected breach	
4.	Suspected designated person (including persons owned or controlled by them)			
	Name of the designated person			

	Name of the person/entity if owned/controlled by a designated person	
5.	What has caused you to know or suspect that the person you are reporting on is a designated person (or is owned/controlled by one)?	
6.	Please provide any information by which the designated person can be identified	
7.	Who do you suspect has committed, or has attempted to commit, the suspected breach?	
8.	Does this information relate to a suspected completed or suspected attempted breach?	
9.	What does the suspected breach involve?	

10.	Are you providing any supporting documents?				
		Economic resource(s)	Financial services	License conditions	Reporting obligations
11.	Other relevant information				
12.	I confirm that all information I have provided in this form is accurate and true to the best of my knowledge.				<hr style="width: 100px; margin-left: auto;"/> <u> X    ✓ </u>

	<p>NAME:</p> <p>DESIGNATION:</p> <p>DATE:</p>

## ANNEXURE 2: SANCTIONS REPORT FORM (external – to be submitted to the Financial Intelligence Centre)

1. This form should be used to report all required information to the Financial Intelligence Centre (**FIC**), including information regarding the suspected designated persons, frozen assets and suspected breaches of financial sanctions.
2. Please note that the information provided in this form may be shared for the purpose of facilitating or ensuring compliance with financial sanctions regulations, in accordance with the FIC's information-sharing powers.
3. The Company's and its employees' financial sanctions reporting and compliance obligations are described in BROKSTOCK SA (PTY) LTD's Anti-Money Laundering, Terrorist and Proliferation Financing Policy (FIC or AML Policy). Please review this Policy carefully prior to completing this form.
4. Please ensure that when you complete this form, you believe that the facts and information provided in this form are accurate and true to the best of your knowledge.
5. Following completion, please e-mail the completed form, including any associated documents, to [pserfontein@brokstock.co.za](mailto:pserfontein@brokstock.co.za) or [compliance@brokstock.co.za](mailto:compliance@brokstock.co.za).

2.	<b>GENERAL INFORMATION</b>			
	Details of the person completing this report			
	Name (including title)			
	Job title			
	Company/organisation			
	Address:			
	Contact number(s)			
	Email address			
	Date submitted (dd/mm/yyyy)			
	Are you submitting this form on behalf of a third party?	Y	N	

	What are you reporting?					
	Suspected designated person		Frozen assets		Suspected breach	
3.	<b>REPORTING A SUSPECTED DESIGNATED PERSON</b>					
	This part should be used to report your knowledge or suspicion that an individual, business or organisation is a designated person and therefore subject to financial sanctions.					
	Your report should include information by which a designated person can be identified.					
	Suspected designated person (including persons owned or controlled by them).					
	Name of the designated person					
	Name of the person/entity if owned/controlled by a designated person					
	Information on which your knowledge or suspicion is based					
	What has caused you to know or suspect that the person you are reporting on is a designated person (or is owned/controlled by one)?					
	Please provide any information by which the designated person can be identified.					

<b>4.</b>	<b>INFORMATION ON FROZEN ASSETS</b>
	This part should be used to report that you have frozen the assets of a designated person.
	Designated person (DP)
	Name of the designated person
	Name of the person/entity if owned/controlled by a designated person
	Please provide information on all funds and economic resources you have frozen.
<b>5.</b>	<b>INFORMATION ABOUT A SUSPECTED BREACH</b>
	This part should be used to report any suspected or known breach of financial sanctions.

	Your report should include all known details in relation to the suspected breach activity. Where information is not known or not applicable, please state.
	Who do you suspect has committed, or has attempted to commit, the suspected breach?
	<b>Summary of facts</b>
	Does this information relate to a suspected completed or suspected attempted breach?
	Financial sanctions regime(s) under which the suspected breach has occurred
	Financial sanctions regime(s)
	Act/Regulation(s) (if known)
	Relevant section(s), article(s), regulation(s) suspected of having been breached (if known)
	<b>Sanctions lists in effect can be found on:</b>

	UN sanctions - <a href="https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list">https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list</a> ;									
	EU sanctions - <a href="https://www.sanctionsmap.eu/#/main">https://www.sanctionsmap.eu/#/main</a> ;									
	UK sanctions - <a href="https://www.gov.uk/government/publications/the-uk-sanctions-list">https://www.gov.uk/government/publications/the-uk-sanctions-list</a> ;									
	OFSI sanctions - <a href="https://www.gov.uk/government/collections/financial-sanctions-regime-specificconsolidated-lists-and-releases">https://www.gov.uk/government/collections/financial-sanctions-regime-specificconsolidated-lists-and-releases</a> ;									
	OFAC sanctions - <a href="https://sanctionssearch.ofac.treas.gov/">https://sanctionssearch.ofac.treas.gov/</a> .									
<b>6.</b>	<b>DETAILS OF SUSPECTED BREACH</b>									
	What does the suspected breach involve:									
	Funds		Economic resource(s)		Financial services		License conditions		Reporting obligations	
	Total value of the suspected breach (actual or estimated)									
	Method(s) of payment and/or transfer									
	Sender information									
	Intermediary information									
	Ultimate beneficiary information									
	Please list all external parties who have been made aware that this information is being passed to the FIC, including any designated persons									

	Has this matter been reported to any other authority?	<input type="checkbox"/> Y	<input type="checkbox"/>	<input type="checkbox"/> N	<input type="checkbox"/>
	Other relevant information				
	Are you providing any supporting documents?	<input type="checkbox"/> Y	<input type="checkbox"/>	<input type="checkbox"/> N	<input type="checkbox"/>
	I confirm that all the information I have provided in this form is accurate and true to the best of my knowledge.				
	<hr/> <input checked="" type="checkbox"/> <input type="checkbox"/>				
	NAME:  DESIGNATION:  DATE:				