Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT)

This policy is organised within the following sections:

1.	Policy Statement
2.	Objective
3.	Scope
4.	Governance and Accountability
5.	Risk-Based Approach
6.	Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)
7.	Sanctions Screening and Compliance Commitment
8.	Ongoing Monitoring and Suspicious Activity Reporting
9.	Training and Capacity Building
10.	Record keeping and Data Retention
11.	Independent Audit and Review
12.	Policy Review and Updates
13.	Zero Tolerance Declaration

1. Policy Statement

Geniusys Group is fully committed to maintaining the highest standards of integrity and compliance in all business dealings. We recognise that Money Laundering (ML) and Terrorism Financing (TF) pose serious threats to global security, financial systems, and our corporate reputation. This policy sets forth a robust framework to prevent, detect, and report ML/TF activities across all operations of Geniusys Group.

2. Objective

This policy aims to:

- Protect Geniusys Group from being misused for illicit financial activities.
- Ensure full regulatory compliance across all jurisdictions of operation.
- Embed a strong culture of ethical conduct and financial transparency.
- Safeguard the interests of stakeholders, clients, partners, and employees.

3. Scope

This policy applies to:

- All entities, subsidiaries, and affiliates under Geniusys Group.
- All directors, officers, employees, and authorised representatives.
- All business relationships and transactions, regardless of geography.

4. Governance and Accountability

A clear governance structure is in place to uphold AML/CFT standards:

Level	Responsibility
• Board of Directors	Ultimate oversight and accountability; policy approval and strategic direction.
• Senior Management	Operational leadership; resource allocation and accountability for compliance.
• Compliance Function	Day-to-day implementation, monitoring, reporting, and regulatory liaison.
• Internal Audit	Independent assessment of framework effectiveness and control adequacy.

The Group maintains a designated AML Compliance Officer, who is responsible for overseeing the implementation of this policy, coordinating group-wide compliance efforts, and ensuring alignment with evolving regulatory and global risk landscapes.

5. Risk-Based Approach

Geniusys Group applies a risk-based approach to identify, assess, and mitigate ML/TF risks based on:

- Customer type and background
- Products and services offered
- Transaction patterns and channels
- Jurisdictional exposure and regulatory complexity

Risk ratings are continuously updated based on internal assessments, regulatory changes, and audit findings.

6. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

Robust CDD procedures are required for all new and existing business relationships:

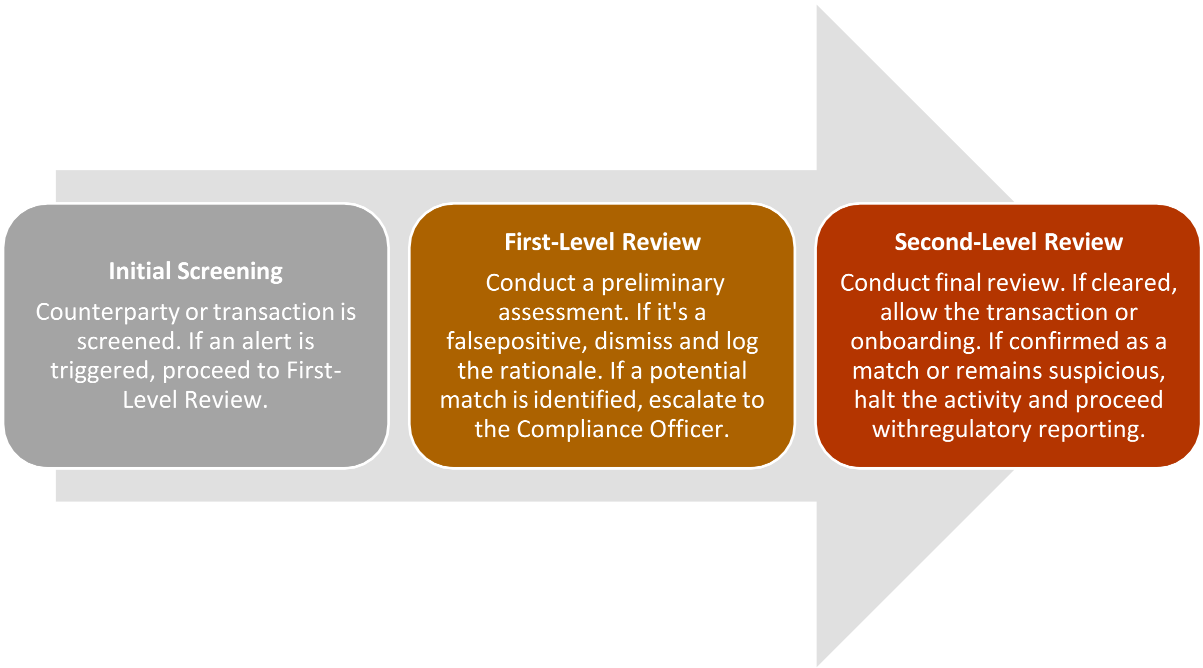
Standard CDD	Enhanced CDD (EDD)
• Identify verification (individual/entity)	High-risk jurisdictions (e.g. FATF grey/blacklisted countries.
• Beneficial ownership disclosure	Politically Exposed Persons and their close associates.
• Business purpose and transaction profile	Unusual or complex ownership structures or transaction behaviour.

EDD measures may include site visits, source of wealth verification, senior management approval, and enhanced monitoring.

7. Sanctions Screening and Compliance Commitment

Geniusys Group recognises the critical role of annual sanctions screening in maintaining an effective AML/CFT framework. As part of our ongoing program development, the Group is committed to establishing appropriate tools, procedures, and escalation protocols to support comprehensive screening of counterparties and transactions against relevant international sanctions and watchlists. Once implemented, these controls will ensure that any potential matches are promptly identified, investigated, and resolved before proceeding with onboarding or transactional activity.

7.1 Escalation Protocol



8. Ongoing Monitoring and Suspicious Activity Reporting

All transactions and customer activity are monitored through a combination of automated tools and human oversight to detect:

- Transaction anomalies
- Structuring/smurfing patterns
- Unjustified changes in behaviour or documentation

Where suspicion arises, internal escalation protocols must be followed without delay. If suspicion is substantiated, the Compliance Officer will file a Suspicious Transaction Report. Employees are protected under whistleblower safeguards when reporting in good faith.

9. Training and Capacity Building

Geniusys Group maintains a dynamic AML/CFT training program that ensures:

- All employees receive annual mandatory training
- High-risk functions (e.g., sales, finance, procurement) receive targeted modules
- New joiners are trained during induction and certified accordingly

The Compliance Department will continuously refresh training content to reflect new typologies, red flags, and jurisdictional risks.

10. Record keeping and Date Retention

The Group retains all relevant documentation for a minimum of seven (7) years, including:

- CDD/EDD files and approvals
- Risk assessments and customer profiles
- STR filings and correspondence
- Internal audit and compliance reviews

All records must be securely stored and retrievable upon regulatory or internal request.

11. Independent Audit and Review

The effectiveness of this policy and the wider AML/CFT framework will be reviewed through:

- Annual internal audits
- Compliance self-assessments
- Independent third-party reviews (where appropriate)
- Regulatory feedback and findings

Findings are reported directly to the Board and used to drive continuous improvement.

12. Policy Review and Updates

This policy will be reviewed at least annually, and more frequently if:

- Regulatory requirements change
- Emerging risks are identified
- Internal or external audit findings warrant revision

Any material updates must be approved by the Board of Directors.

13. Zero Tolerance Declaration

Geniusys Group maintains a zero-tolerance stance towards money laundering and terrorism financing. Any employee, agent, or business partner found complicit or negligent in AML/CFT obligations may face:

- Disciplinary action, up to and including termination
- Referral to law enforcement and regulatory authorities
- Civil or criminal liability

Appendix 1: Due Diligence Assessment for New Vendor/Customer

Due Diligence Assessment for New Vendor/Customer

Organization Name:	
Contact Person:	
Position:	
Address:	
Phone Number:	
Email Address:	
Date of Assessment:	

Organizational Information

Question	Yes	No	N/A	Comments
Legal status verified? (e.g., Company registration, licenses)	☐	☐	☐	
Date of Establishment	☐	☐	☐	
Mission and objectives aligned with our values?	☐	☐	☐	
History of operations and reputation evaluated?	☐	☐	☐	

Financial and Legal Compliance

Annual Financial Statements Reviewed? (if applicable)	☐	☐	☐	
Compliance with relevant laws and regulations checked?	☐	☐	☐	
Financial audits conducted regularly?	☐	☐	☐	
Any pending legal issues or major liabilities?	☐	☐	☐	

Business & Program Evaluation

Products and services reviewed and evaluated?	☐	☐	☐	
Evidence of effective use of previous contracts/partnerships?	☐	☐	☐	
Expected business outcomes and mutual benefits identified?	☐	☐	☐	

Ethical Considerations

No evidence of mismanagement or fraud?	☐	☐	☐	
No conflicts of interest identified?	☐	☐	☐	
Ethical and responsible practices confirmed?	☐	☐	☐	

Transparency and Accountability

Question	Yes	No	N/A	Comments
Contact for follow-up	☐	☐	☐	
Clear timelines for communication and deliverables?	☐	☐	☐	

Strategic Alignment
Operational Capacity

Sufficient infrastructure for scale?	☐	☐	☐	
Adequate workforce capacity for growth?	☐	☐	☐	
Proven ability to meet delivery and quality standards?	☐	☐	☐	

Feedback and Follow-up

Post-engagement evaluation plan to assess outcomes in place?	☐	☐	☐	
Mechanisms for regular feedback and communication confirmed?	☐	☐	☐	

Assessment Completed By:	
Title:	
Date:	
Signature:	

Appendix 2: Due Diligence Assessment for Donation/Sponsorship Recipients

Due Diligence Assessment for Donation/Sponsorship Recipients

Organization/Individual Name:	
Contact Person:	
Position:	
Address:	
Phone Number:	
Email Address:	
Date of Assessment:	

Organizational Information

Question	Yes	No	N/A	Comments
Legal status verified? (e.g., nonprofit status, registered charity)				
Mission and objectives aligned with our values?				
History of operations and reputation evaluated?				

Financial and Legal Compliance

Annual Financial Statements Reviewed? (if applicable)				
Compliance with relevant laws and regulations checked?				
Financial audits conducted regularly?				

Program and Impact Evaluation

Description of programs and services reviewed?				
Evidence of effective use of previous donations/sponsorship?				
Expected outcomes and impact of proposed donation/sponsorship				

Ethical Considerations

No evidence of mismanagement or fraud?				
No conflicts of interest identified?				
Ethical and responsible use of fund ensured?				

Transparency and Accountability

Contact information for follow-up and reporting?				
Clear reporting timelines established?				

Alignment With Strategic Goals

Strategic Alignment: Does the recipient's mission and objectives align with organization's strategic goals and areas of focus?				
Contributions to long-term impact: Does the partnership contribute to long-term goals?				

Volunteer Engagement

Volunteer Program: Does the organization have a striuctured volunteer program?				
Volunteer Management: Are volunteers managed effectively and given adequate support and training?				

Feedback and Follow-up

Post-Support Evaluation: Is there a plan for post-support evaluation to assess the effectiveness and impact of the donation or sponsorship?				
Follow-Up Mechanisms: Are there mechanisms for ongoing communication and follow-up with the recipient to ensure accountability and address any issues?				

Assessment Completed By:	
Title:	
Date:	
Signature:	

Appendix 3: Due Diligence Assessment for New Employee

Due Diligence Assessment for New Employee

Owner(s):	Human Resources Department
Assessment With:	
Date:	

Employee and HR Assessment

Background Checks

Question	Yes	No	N/A	Comments
Background check completed?				
Reference Checks Conducted?				
Verification of educational qualifications?				
Social media and online presence check?				
Criminal record check completed?				
Credit history check (if applicable)?				

Documentation and Polices

Employee handbook provided?				
Written job description available?				
Employment contract signed?				
Orientation/Induction training completed?				
Company policies acknowledged?				

Employee Wellbeing and Environment

Medical checkup needed?				
Onboarding process completed?				
Ergonomics and workplace setup assessed?				

Legal and Compliance

Legal authorization to work verified?				
Compliance with labour laws and regulations checked?				

Confidentiality and Security

Data protection and confidentiality policies explained?				
Physical access to workplace restricted (e.g., ID cards)?				
Password management policy explained?				

Miscellaneous

Employee's financial behaviour (living beyond means)?				
Family or friend relations in the workplace (potential conflicts of interest)?				
Any previous employment disputes or legal actions?				
Conflict of interest declaration signed?				
Monitoring of social and professional conduct (if applicable)?				
Community involvement or volunteer work?				

Completed By:	
Title:	
Date:	
Signature:	

Suspicious Transaction Report (STR)

Reporting Entity:	
Date of Report:	

Reported By:	
Name:	
Designation:	
Email:	
Phone:	

Details of the Subject (Individual or Entity):	
Name:	
Registration No / IC No:	
Address:	
Nationality/Country of Incorporation:	
Nature of Business:	

Nature of the Suspicion:

Transaction Details:	
Date of Transaction:	
Transaction Type:	
Description:	
Reason Suspended:	

Action Taken: