Know Your Customer (KYC) Policy

of PARTNUGGET CAR PARTS TRADING DWC LLC

1. Purpose of the Policy

This Policy outlines the guiding principles, procedures, and responsibilities for the implementation of a robust Know Your Customer (KYC) framework within **PARTNUGGET CAR PARTS TRADING DWC LLC** ("RESELLER OF RECORD"). It is intended to ensure compliance with applicable **Anti-Money Laundering (AML)**, **Counter-Terrorism Financing (CTF)**, and **international sanctions** frameworks, in accordance with UAE legislation, global FATF standards, and best industry practices.

This Policy seeks to:

- Deter and detect the misuse of this website for illicit purposes.
- Safeguard the RESELLER OF RECORD from financial crimes and reputational damage.
- Promote a culture of compliance and risk-awareness within all functional areas.

2. Scope of Application

This Policy applies to all interacting with this website, including but not limited to:

- **Buyers**: Entities purchasing goods, services, or inventory via this website.
- **Suppliers**: Entities listing or selling goods, including both manufacturers and distributors.
- **Logistics and Delivery Providers**: Organizations providing shipment, customs, or freight forwarding services.
- **Partners and Affiliates**: Entities involved in strategic collaborations or contractual relationships with RESELLER OF RECORD.

Natural persons are onboarded only in cases explicitly allowed by law or upon special authorization by the Compliance Officer.

3. Core KYC Principles

- **Customer Identification and Verification (CIV):** Verification of identity using government-issued documentation and corporate credentials.
- **Enhanced Due Diligence (EDD):** Applied in high-risk situations, including high-value transactions, complex ownership structures, or high-risk geographies.
- **Risk-Based Approach (RBA):** Risk level determines the depth of scrutiny, frequency of monitoring, and reporting obligations.
- **Transparency of Ultimate Beneficial Ownership (UBO):** All controlling individuals must be disclosed and validated.

- **Ongoing Monitoring:** Surveillance continues throughout the business relationship, not only at onboarding.
- **Confidentiality & Data Protection:** All information is processed in compliance with the **UAE PDPL**, **EU GDPR**, and other applicable privacy laws.
- **Zero-Tolerance Policy:** Violations of KYC policy result in regulatory notifications, account restrictions, or offboarding.

4. Stages of the KYC Process

4.1. Data Collection

Mandatory documents include:

- Certificate of Incorporation;
- Articles of Association or equivalent formation documents;
- Valid passport/ID of the authorized representative;
- Proof of authority (Power of Attorney, Board Resolution, or appointment letter);
- Trade licenses and regulatory approvals;
- Bank account ownership proof (letter or recent bank statement);
- Current physical address and contact details.

4.2. Data Verification

All documentation is verified through:

- Cross-referencing with government or commercial registries;
- Independent third-party screening tools (e.g., World-Check, Dow Jones Risk & Compliance);
- Video interviews for enhanced authenticity when required;
- Screening for sanctions, adverse media, and PEP status.

4.3. Transaction Monitoring & Risk Assessment

- **Automated Monitoring:** Real-time system-based triggers for anomalous activity (unusual volumes, split transactions, etc.).
- **Behavioral Profiling:** Establishing a transaction baseline to detect deviations.
- **Escalation Procedures:** High-risk transactions are subject to manual review and potential suspension.

4.4. Risk-Based Decision-Making

- **Greenlight (Low Risk):** Immediate access after standard verification.
- **Yellowlight (Medium Risk):** Limited access pending further review.
- **Redlight (High Risk):** Denial of onboarding or immediate termination if flagged.
- All outcomes are logged, time-stamped, and auditable.

5. Ongoing Monitoring and Reassessment

- **Periodic Reviews:** Risk-based periodicity (e.g., 6 months for high-risk, 12 months for standard-risk).
- **Trigger-Based Reviews:** Change in UBO, media alerts, suspicious activity, etc.
- **Technology-Assisted Alerts:** IP geofencing, behavioral deviation, and device fingerprinting trigger automatic reviews.

6. Data Retention and Security

- Data is encrypted at rest and in transit using AES-256 encryption.
- Tiered access control ensures only authorized staff access KYC data.
- All actions are logged with immutable audit trails.
- **Minimum Retention:** 5 years from last activity or end of contractual relationship, per AML laws.

7. Roles and Responsibilities

- **Visitors and users of this website:** Responsible for truthfully providing all requested information and promptly reporting any changes.
- **Compliance Officer:** Oversees end-to-end KYC, approves high-risk cases, manages escalations, and ensures system integrity.
- **Legal Team:** Drafts legal clauses, interprets UAE and international regulations, and supports enforcement actions.
- **Technology Team:** Ensures secure KYC workflows, integrates AML solutions, and maintains logs.
- **Operations & Support:** Guides users through onboarding, document submission, and remediation steps.

8. Review and Policy Governance

This Policy is subject to:

- **Annual Review**: Led by the Compliance Officer and Legal Department.
- **Interim Amendments**: Promptly after major legal or technological changes, FATF recommendations, or post-audit findings.
- **Board Approval**: Significant structural changes must be presented for senior management review and approval.

9. Enforcement and Sanctions

Non-compliance with this Policy may result in:

- Immediate account freezing;
- Termination of contractual engagement;
- Reporting to the UAE Financial Intelligence Unit (FIU), Central Bank, or other relevant regulators;
- Civil or criminal liability depending on the nature of the breach.