SUMNER GLOBAL HUB

AML/CTF Policy for Defence Sector Business

Introduction This policy sets out the controls and procedures implemented to prevent the business from being used for money laundering, terrorist financing, sanctions evasion, and the illicit procurement of defence or dual-use goods

The organisation is committed to full compliance with applicable UK legislation, guidance from the Financial Conduct Authority, international standards set by the Financial Action Task Force, and defence/export control regulations administered by the Ministry of Defence and the UK Export Control Joint Unit.

This policy is relevant to all directors, all employees, contractors, consultants, customers, agency workers, freelancers, temporary staff, suppliers, intermediaries, and service providers acting on behalf of the Company; and any third-party undertaking business activities for or on behalf of Sumner Global Hub Limited. It covers all transactions involving defence, security, dual-use, or sensitive technologies, and all jurisdictions in which the business operates

Every individual covered by this policy is responsible for complying with its requirements.

Implementing the Policy
Sumner Global Hub Limited employees will be informed of this policy and will be provided with training appropriate to their needs and responsibilities. All those who act on the Sumner Global Hub Limited's behalf will be informed of this policy and will be expected to pay due regard to it when conducting business on Sumner Global Hub Limited's behalf.

Reporting Complaints or Policy Breaches
Any suspicion of a breach of this policy must be immediately reported to: Laura Chamberlain.

Policy Owner: Compliance Department – Compliance Officer

Approved By: Board of Directors **Version** 1.0

Effective Date: June 15, 2026 **Review Date**: June 15, 2027

This policy is considered a working document, which is subject to regular review. It will be reviewed at least annually, when regulatory changes occur, and following any significant compliance incident.

Risk-Based Approach
The company applies a **risk-based approach (RBA)**, considering high-risk indicators specific to defence sector (e.g., military or dual-use end users, complex procurement chains or intermediaries, unusual funding structures [i.e., third-country payments, shell entities],

transactions involving sanctioned or high-risk jurisdictions, and requests lacking clear end-use or end-user certification).

Risk ratings:

- Low risk → standard due diligence
- Medium risk → enhanced monitoring
- High risk → Enhanced Due Diligence (EDD) + senior approval

Customer, Supplier & Partner Due Diligence (CDD)

Before onboarding any party, the organisation must:

- Verify legal identity (company registration, ownership structure)
- Identify Ultimate Beneficial Owners (UBOs)
- Confirm nature of business and legitimacy of operations
- Assess relevance to defence supply chains
- Screen against sanctions and watchlists

No relationship may begin without completed CDD approval.

Enhanced Due Diligence (EDD)

EDD is mandatory for:

- Defence contractors and subcontractors
- Government-linked entities in high-risk regions
- Politically Exposed Persons (PEPs)
- Complex ownership structures (multi-layered offshore entities)
- High-value or sensitive procurement contracts

EDD measures include:

- Source of funds and source of wealth verification
- End-user and end-use certification (mandatory in defence transactions)
- Site visits or independent verification (where appropriate)
- Senior compliance officer approval

Sanctions & Export Controls Compliance

The organisation strictly complies with UK Sanctions Lists; UN, EU, and US sanctions (where applicable to operations); and export control regimes (including military and dual-use goods).

No goods, services, or technical data may be transferred without:

- Export licence approval, where required
- Screening of all parties (e.g., buyer, intermediary, end user)
- Verification of lawful end use

Transaction Monitoring

All transactions must be monitored for:

- Unusual payment structures (e.g., split payments, layering)
- Third-party payments without justification

- Overpayments or refunds to unrelated accounts
- Discrepancies between contract value and payment flows
- Rapid movement of funds across jurisdictions

Any suspicious activity must be escalated immediately.

Suspicious Activity Reporting (SAR)
Employees must report suspicions to the designated Money Laundering Reporting Officer (MLRO). The MLRO will review internal reports, determine whether external reporting is required to the National Crime Agency (NCA), and ensure strict confidentiality.

Tipping off is strictly prohibited.

Record Keeping
The organisation will retain due diligence documentation, contracts and procurement records, transaction records, compliance decisions, and risk assessments.

Retention period is a minimum of **5 years** (or longer if legally required).

Governance & Responsibilities
The Board of Directors has the overall responsibility for AML/CTF compliance. The MLRO has oversight of suspicious activity reporting and regulatory liaison. The Compliance Team is responsible for risk assessments, onboarding approvals, and monitoring. All employees have to be in mandatory compliance with policy and training obligations.

Training
Mandatory training includes:
- AML/CTF awareness
- Defence-sector-specific risks (dual-use goods, procurement fraud, sanctions evasion)
- Identification of suspicious indicators
- Reporting procedures

Training is conducted at onboarding, annually thereafter, and when regulations change.

Third Parties, Agents & Intermediaries
Due to elevated risk in defence procurement:
- All agents must undergo full due diligence.
- Commission structures must be transparent and justified.
- Use of intermediaries in high-risk jurisdictions requires senior approval.
- No undisclosed subcontracting is permitted.

Red Flags (Defence Sector Specific)
- Requests to obscure end-user identity
- Refusal to provide end-use certification

- Complex routing through multiple jurisdictions
- Pressure for unusual payment terms
- Use of newly formed shell companies in procurement
- Unusual urgency inconsistent with legitimate defence procurement cycles

Non-Compliance Consequences

Failure to comply may result in disciplinary action or termination, contract termination, reporting to regulators or law enforcement, civil or criminal penalties, or loss of export privileges.