



ANDRO SECURE GROUP

I R E L A N D

PROTECTING YOUR ASSETS
WITH INTEGRITY AND EXCELLENCE



COMMODITY TRADING COMPLIANCE POLICY

Document Title	Commodity Trading Compliance Policy
Applicable Entity	Andro Secure Group Ltd (Ireland), Irish Registration No. 767962, and its trading divisions and affiliates engaged in commodity trading activity
Document Owner	Compliance Officer / Money Laundering Reporting Officer (MLRO), Andro Secure Group Ltd
Approval Authority	Managing Director, Andro Secure Group, on the recommendation of the Compliance Officer
Version	1.0
Effective Date	To be inserted upon Board / Managing Director approval
Next Scheduled Review	12 months from Effective Date, or earlier upon material regulatory change
Classification	Internal — Controlled Document. Available to regulators, auditors, and trading counterparties on request

Version Control

Version	Date	Author	Summary of Changes
0.1	Drafting stage	Compliance Function	Initial draft prepared for internal legal and management review
1.0	See Effective Date above	Compliance Officer, approved by Managing Director	First Board/MD-approved version; full policy issued for firm-wide implementation

Approval Statement

This policy has been reviewed and approved by the Managing Director of Andro Secure Group, acting as the Approval Authority for compliance policy issued by the Company. Approval confirms that the policy reflects the Company's operating model, has been assessed against applicable Irish and EU legal and regulatory requirements, and is authorised for firm-wide implementation from the Effective Date stated above.

Approved by: C.J. (Christo) Rabie



Position: Managing Director Date: 19 August 2026



Table of Contents

- 1. Introduction, Purpose and Scope**
 - 2. Regulatory Framework: Irish and EU Financial Services Law**
 - 3. Anti-Money Laundering, Countering the Financing of Terrorism, and Sanctions**
 - 4. Market Abuse, Insider Dealing, and Market Manipulation**
 - 5. Environmental, Social, and Sustainability Compliance**
 - 6. Position Limits, Counterparty Exposure, and Risk Management**
 - 7. Client and Counterparty Onboarding and Due Diligence**
 - 8. Record-Keeping and Documentation**
 - 9. Conflicts of Interest**
 - 10. Compliance Monitoring, Breach Detection, and Regulatory Reporting**
 - 11. Training, Competence, and Certification**
 - 12. Enforcement, Disciplinary Procedures, and Remediation**
 - 13. Policy Governance, Review, and Amendment**
- Appendices A–H



1. Introduction, Purpose and Scope

1.1 Purpose

This Compliance Policy ("the Policy") sets out the framework by which Andro Secure Group Ltd ("Andro Secure", "the Company") conducts commodity trading activity in a manner that is lawful, ethical, and consistent with Irish and European Union regulatory requirements. It applies to trading in precious metals, energy products, and agricultural commodities, whether conducted on a spot (physical delivery) basis or through commodity derivatives, and whether executed on the Company's own account, on behalf of clients, or as an intermediary arranging transactions between counterparties.

The Policy is written to be used and understood by compliance officers, legal advisers, trading staff, senior management, external auditors, regulators, and trading counterparties. Where a regulatory term is used for the first time, a plain-language explanation is provided alongside it.

1.2 Scope of Application

This Policy applies to all directors, officers, and employees of Andro Secure Group Ltd, and to any contractor, agent, or introduced business partner who conducts commodity trading activity for or on behalf of the Company, in any jurisdiction in which the Company operates or has operational presence, including but not limited to Ireland, the United Kingdom, Spain, South Africa, and the United States. Where local law in a non-EU jurisdiction imposes a stricter standard than this Policy, the stricter standard applies to activity in that jurisdiction.

The Policy covers, at a minimum, the following commodity classes and the associated derivative instruments where the Company trades or intends to trade them:

- Precious metals — physical gold, silver, platinum, and palladium, and related forwards, swaps, and options;
- Energy products — crude oil, refined products, natural gas, and power, and related derivatives; and
- Agricultural commodities — soft commodities and grains, and related derivatives, together with any related financing, storage, transport, and documentary trade instruments (including standby letters of credit, bills of lading, and warehouse receipts) used to support these activities.

1.3 Status of the Company and Applicability of Regulated Activity

Andro Secure Group Ltd.'s core business is physical and operational risk management, including maritime security, executive protection, high-value transport, and aviation security. Where the Company or an affiliated trading division engages in commodity trading — including introducing, structuring, financing, or executing trades in precious metals, energy, or agricultural commodities, or in commodity derivatives — this Policy applies in full, and the Company will assess, transaction by transaction and activity by activity, whether that trading activity brings it within the scope of MiFID II as an "investment firm" carrying out "investment services" in "financial instruments", within the scope of EMIR as a counterparty to derivative contracts, or within scope only of general commercial, AML, and sanctions law applicable to physical commodity dealing. Section 2 sets out how that assessment is made and documented.

1.4 Key Definitions

- "Central Bank" or "CBI" means the Central Bank of Ireland, Ireland's competent authority for financial services regulation and the supervisor of MiFID investment firms, payment and e-money institutions, and (for AML/CFT purposes) designated persons in the financial sector.
- "MiFID II" means Directive 2014/65/EU on markets in financial instruments, as implemented in Ireland principally through the European Union (Markets in Financial Instruments) Regulations 2017 (S.I. No. 375 of 2017), together with the related Markets in Financial Instruments Regulation (EU) No 600/2014 ("MiFIR").



- "EMIR" means Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories, as amended, which governs clearing obligations, risk mitigation, and reporting for derivative contracts, including many commodity derivatives.
- "MAR" means the Market Abuse Regulation (EU) No 596/2014, which prohibits insider dealing, unlawful disclosure of inside information, and market manipulation, and which applies to financial instruments (including commodity derivatives) and, in defined circumstances, to related spot commodity contracts.
- "AML/CFT" means anti-money laundering and countering the financing of terrorism, governed in Ireland principally by the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended ("the CJA 2010"), which transposes the EU Anti-Money Laundering Directives.
- "Designated Person" is the term used in the CJA 2010 for an entity subject to Irish AML/CFT obligations; Andro Secure treats itself as a Designated Person for the purposes of this Policy in respect of all commodity trading and related financial activity, irrespective of whether a given transaction also falls within MiFID II.
- "Sanctions" means restrictive measures adopted by the United Nations, the European Union (through Council Regulations), Ireland, and — where the Company's activities have a US nexus — the United States Office of Foreign Assets Control ("OFAC"), and any other jurisdiction in which the Company operates.
- "Inside Information" has the meaning given in Article 7 of MAR: information of a precise nature, not generally available, relating directly or indirectly to a financial instrument or related spot commodity contract, which, if made public, would be likely to have a significant effect on prices.

2. Regulatory Framework: Irish and EU Financial Services Law

Policy Statement

Andro Secure will identify, document, and keep current the full inventory of Irish and EU legal and regulatory obligations that apply to its commodity trading activities, and will operate a documented process for classifying each trading activity against that inventory before it is undertaken.

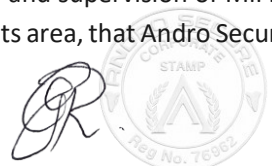
The Company recognises that commodity trading regulation in the EU operates on a spectrum: purely physical (spot) trading in precious metals, energy, or agricultural commodities is generally outside MiFID II and EMIR, whereas commodity derivatives (futures, forwards for financial purposes, options, and swaps) fall within one or both regimes depending on characteristics such as standardisation, settlement method, trading venue, and the availability of exemptions (including the MiFID II Annex I Section C(6) and C(7) "ancillary activity" tests for physically settled forwards and the commercial hedging exemptions in EMIR).

Regulatory Rationale

MiFID II (Directive 2014/65/EU) and MiFIR (Regulation (EU) No 600/2014), transposed in Ireland through the European Union (Markets in Financial Instruments) Regulations 2017, regulate the provision of investment services in financial instruments, which include most standardised and cash-settled commodity derivatives. Firms providing MiFID investment services in Ireland must generally be authorised by the Central Bank of Ireland, unless an exemption applies.

EMIR (Regulation (EU) No 648/2012, as amended by EMIR Refit and EMIR 3.0) imposes clearing, reporting, and risk-mitigation obligations on counterparties to OTC derivative contracts, including many commodity derivatives, with the scope of obligations depending on whether a counterparty is classified as a Financial Counterparty ("FC") or Non-Financial Counterparty ("NFC"), and, for NFCs, whether clearing thresholds are exceeded.

The Central Bank of Ireland is the competent authority responsible for the authorisation and supervision of MiFID investment firms in Ireland and publishes guidance, including on the Central Bank's Markets area, that Andro Secure will monitor for developments relevant to its trading activity.



Where the Company's activity remains purely physical/spot commodity dealing, MiFID II and EMIR obligations as such do not typically apply, but the Company remains subject to general Irish company and commercial law, sanctions law, and AML/CFT law addressed in Sections 3 and elsewhere in this Policy.

Implementation Procedures

- 2.1 The** Compliance Officer will maintain a Regulatory Perimeter Assessment for each new commodity or product line before trading begins, documenting whether the activity is (a) pure physical/spot trading, (b) a commodity derivative falling within an available exemption, or (c) a commodity derivative requiring MiFID II authorisation or falling within EMIR scope, with the underlying analysis retained on file (see Appendix A).
- 2.2 Where** an assessment concludes that a proposed activity would require MiFID II authorisation that the Company does not hold, that activity will not proceed until either the necessary authorisation is obtained from the Central Bank of Ireland or the activity is restructured to fall within an applicable exemption, confirmed in writing by external legal counsel.
- 2.3 For** any derivative contracts the Company enters into, the Compliance Officer will determine EMIR counterparty classification (FC/NFC+/NFC-), monitor notional positions against the relevant clearing thresholds by asset class, and ensure risk-mitigation obligations (timely confirmation, portfolio reconciliation, portfolio compression where applicable, and dispute resolution procedures) and trade reporting to a registered or recognised trade repository are operating as required.
- 2.4 The** Compliance Officer will subscribe to Central Bank of Ireland and ESMA (European Securities and Markets Authority) regulatory update channels and will brief the Managing Director and trading staff on material changes at least quarterly, and immediately where a change affects a live trading activity.
- 2.5 The** Company will obtain external legal or regulatory advice before entering into a materially new commodity product line, a new derivative type, or a new jurisdiction of operation.

Responsible Parties: Compliance Officer (regulatory perimeter assessments and monitoring); Managing Director (final decision on new regulated activity); External Legal Counsel (formal opinions on authorisation and exemption questions).

3. Anti-Money Laundering, Countering the Financing of Terrorism, and Sanctions

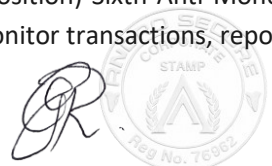
Policy Statement

Andro Secure will not knowingly facilitate and will take all reasonable and proportionate steps to prevent, money laundering, terrorist financing, proliferation financing, or the circumvention of sanctions, in connection with any commodity trading activity, and will treat itself as a Designated Person under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended, for all such activity.

The Company operates a risk-based AML/CFT programme calibrated to the higher inherent money-laundering and sanctions risk associated with cross-border commodity trading, precious metals, and trade finance instruments, including standby letters of credit.

Regulatory Rationale

The CJA 2010 (as amended, transposing the EU's Fourth, Fifth, and (on further transposition) Sixth Anti-Money Laundering Directives) requires Designated Persons to apply customer due diligence, monitor transactions, report



suspicious transactions to the Financial Intelligence Unit Ireland (FIU Ireland) and the Revenue Commissioners, maintain records, and provide AML/CFT training to staff.

EU sanctions are directly applicable in Ireland through Council Regulations and are given further domestic effect through the Financial Sanctions Act and related statutory instruments; breach of financial sanctions is a serious criminal and regulatory matter, and precious metals, energy, and agricultural commodity trade are sectors specifically targeted by EU and UN sanctions regimes.

Where trading activity has a US nexus (US-dollar settlement, US counterparties, or US persons involved), OFAC sanctions and secondary sanctions exposure must also be assessed, notwithstanding that the Company is not a US entity.

Beneficial ownership transparency obligations under the EU framework and the Irish Central Register of Beneficial Ownership regime require verification of the natural persons who ultimately own or control corporate counterparties.

Implementation Procedures

- 3.1 The** Company will appoint a Money Laundering Reporting Officer (MLRO), who may also act as the Compliance Officer, responsible for the design, operation, and continuous improvement of the AML/CFT programme, and for acting as the reporting point of contact with FIU Ireland.
- 3.2 The** Company will conduct and document a Business-Wide AML/CFT Risk Assessment at least annually, and on any material change to products, geographies, or counterparty base, covering commodity, geographic, delivery channel, and customer risk factors specific to precious metals, energy, and agricultural trading.
- 3.3 Every** counterparty, whether a client, supplier, buyer, financing bank, or intermediary, will be screened against applicable EU, UN, Irish, OFAC, and other relevant consolidated sanctions and asset-freeze lists prior to onboarding, before execution of any transaction, and on an ongoing basis (including automated re-screening against list updates), with positive matches escalated to the MLRO before any further action is taken.
- 3.4 Beneficial** ownership of corporate and trust counterparties will be identified and verified to at least the 25% direct or indirect ownership/control threshold (or lower where risk indicators warrant), cross-checked where available against the Irish Central Register of Beneficial Ownership or the equivalent register in the counterparty's home jurisdiction.
- 3.5 Transactions** will be monitored for red flags associated with commodity trade-based money laundering, including under- or over-invoicing, mismatched quantities or grades, circular or unnecessarily complex intermediary chains, unusual use of standby letters of credit or bank guarantees, counterparties newly incorporated with no trading history for the volumes proposed, and payment instructions inconsistent with the counterparty's registered details.
- 3.6 Where** suspicion of money laundering or terrorist financing arises, the MLRO will file a Suspicious Transaction Report (STR) with FIU Ireland and the Revenue Commissioners without delay, and the transaction will not proceed (or will be held, where legally permissible) pending clearance, consistent with the CJA 2010 "tipping-off" prohibition, which restricts disclosure of the fact or content of a report to the counterparty or unauthorised third parties.
- 3.7 The** Company will retain a documented sanctions escalation procedure distinguishing (a) list matches requiring immediate transaction freeze and notification to the Department of Foreign Affairs / the relevant competent authority, from (b) false positives resolved through documented due diligence.

Responsible Parties: Money Laundering Reporting Officer / Compliance Officer (programme ownership, screening escalation, STR filing); Trading and Onboarding Staff (first-line screening and red-flag identification); Managing Director (resourcing and escalation of material sanctions exposure).



4. Market Abuse, Insider Dealing, and Market Manipulation

Policy Statement

Andro Secure prohibits insider dealing, unlawful disclosure of inside information, and market manipulation by any director, officer, employee, or agent, in relation to any financial instrument (including commodity derivatives) and, where applicable, related spot commodity contracts, and will apply MAR-consistent standards even where a specific transaction falls outside MAR's formal scope, as a matter of good governance.

Personnel with access to non-public, price-sensitive information relating to the Company's own trading positions, client orders, or physical logistics (such as shipment timing or volumes) must treat that information as confidential and must not trade on it, disclose it, or allow it to influence recommendations to others, other than in the proper course of their duties.

Regulatory Rationale

MAR (Regulation (EU) No 596/2014) prohibits insider dealing, recommending or inducing another person to engage in insider dealing, unlawful disclosure of inside information, and market manipulation, and applies to financial instruments traded on EU trading venues and, importantly for commodity traders, to related spot commodity contracts where the misconduct affects, or is likely to affect, the price of a financial instrument (and vice versa) — this is often described as the MAR "commodity link".

MAR contains commodity-specific manipulation examples, including disseminating false or misleading information about supply, demand, or price of a commodity, and using benchmark-related conduct to distort prices, both of direct relevance to physical energy, metals, and agricultural markets.

MiFID II complements MAR through organisational requirements for firms providing investment services, including systems to detect and report suspicious orders and transactions.

Implementation Procedures

- 4.1 The** Company will maintain, and periodically update, an Inside Information and Market Abuse Procedure identifying the categories of information within the Company's operations that could constitute inside information (for example, undisclosed large physical shipments, pending financing arrangements, or material counterparty developments), and the personnel who may have access to it.
- 4.2 Access** to inside information will be restricted on a need-to-know basis, and where inside information exists, the Compliance Officer will maintain an insider list recording the individuals with access, the reason for access, and the dates access was granted and revoked, consistent with MAR Article 18 practice.
- 4.3 Personal** account dealing by staff with access to inside information, or in instruments related to commodities the Company actively trades, is prohibited without prior clearance from the Compliance Officer, and staff must disclose any personal or family trading interests in relevant markets.
- 4.4 Trading** staff will not place orders or make trades intended to give a false or misleading impression of supply, demand, or price ("spoofing", "layering", "wash trading", or similar conduct), and will not disseminate information they know or ought to know to be false or misleading about a commodity's supply, demand, or price.
- 4.5 Where** the Company reasonably suspects that an order or transaction (its own, a client's, or a counterparty's) may constitute insider dealing or market manipulation, the Compliance Officer will assess the matter and, where warranted, file a Suspicious Transaction and Order Report (STOR) with the Central Bank of Ireland without delay.
- 4.6 Communications** relating to trading (calls, messages, correspondence) will be retained in accordance with Section 8 of this Policy and will be periodically reviewed on a risk basis for indicators of market abuse.

Responsible Parties: Compliance Officer (insider lists, STOR filings, surveillance); Trading Staff (day-to-day conduct and escalation of suspicious counterparty behaviour); Managing Director (oversight of market conduct culture).

5. Environmental, Social, and Sustainability Compliance

Policy Statement

Andro Secure will conduct commodity trading in a manner that has regard to applicable environmental, social, and governance ("ESG") laws and standards, including responsible sourcing expectations for precious metals, environmental and emissions-related obligations relevant to energy trading, and sustainability-related disclosure obligations that apply to the Company or that counterparties reasonably require as a condition of doing business.

The Company will not knowingly trade precious metals, energy products, or agricultural commodities sourced from conflict-affected or high-risk areas in a manner inconsistent with recognised responsible sourcing standards and will apply enhanced due diligence to counterparties and supply chains presenting elevated ESG risk.

Regulatory Rationale

For precious metals, the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas sets the internationally recognised standard for supply-chain due diligence and is referenced by industry bodies such as the London Bullion Market Association (LBMA) Responsible Sourcing Programme, which the Company will have regard to where it trades LBMA-referenced metals or deals with LBMA-accredited counterparties.

For energy trading, EU climate and energy legislation (including the EU Emissions Trading System framework, methane and energy efficiency measures, and evolving due diligence legislation) may impose direct or counterparty-driven obligations relevant to the Company's energy-related activity.

The EU Corporate Sustainability Due Diligence Directive and related supply-chain legislation, together with the EU Deforestation Regulation (relevant to certain agricultural commodities), reflect a broader EU direction of travel toward mandatory supply-chain sustainability due diligence that the Company will monitor for direct or indirect applicability (including as a counterparty requirement imposed by larger trading partners and financing banks) as thresholds and timelines are finalised.

Given Andro Secure's core business in physical and maritime security, the Company will also have regard to environmental and safety standards applicable to the transport, storage, and handling of energy and agricultural commodities under its logistics and security contracts.

Implementation Procedures

- 5.1 The** Compliance Officer will maintain a Responsible Sourcing and ESG Due Diligence checklist applied to new precious metals counterparties and supply chains, addressing origin, chain of custody documentation, and any conflict-mineral or high-risk-area indicators.
- 5.2 Counterparty** due diligence (Section 6) will include an ESG risk flag, escalated for enhanced review where a counterparty operates in, or sources from, a jurisdiction or sector with recognised elevated ESG or human-rights risk.
- 5.3 The** Company will retain documentary evidence of origin, chain of custody, and (where applicable) responsible sourcing certification for precious metals transactions, and will decline to proceed with transactions where credible red flags of conflict-linked or otherwise non-compliant sourcing cannot be resolved.



5.4 The Compliance Officer will maintain a watching brief on incoming EU sustainability due diligence and disclosure legislation relevant to commodity trading and will brief the Managing Director annually, or sooner if a new obligation is confirmed as applicable to the Company.

5.5 Where a counterparty, bank, or trading partner (such as Katradis Group or other institutional counterparties) requires ESG representations, certifications, or reporting as a condition of the relationship, the Compliance Officer will coordinate the Company's response and ensure representations made are accurate and evidenced.

Responsible Parties: Compliance Officer (ESG due diligence framework and monitoring); Trading Staff (origin and chain-of-custody documentation at point of transaction); Managing Director (counterparty-level ESG commitments and representations).

6. Position Limits, Counterparty Exposure, and Risk Management

Policy Statement

Andro Secure will operate within defined position limits, counterparty exposure limits, and concentration limits for all commodity trading activity, calibrated to the Company's capital base, risk appetite, and (where applicable) regulatory position-limit obligations, and will not exceed applicable regulatory position limits for commodity derivatives subject to such limits.

Risk limits will be set and approved by the Managing Director on the recommendation of the Compliance/Risk function, monitored on an ongoing basis, and escalated immediately upon breach or near-breach.

Regulatory Rationale

MiFID II (as amended) provides for position limits and position management controls on commodity derivatives, applied by national competent authorities including the Central Bank of Ireland and, for certain agricultural commodity derivatives, subject to specific EU-harmonised limits; trading venues also impose their own position management controls.

EMIR requires counterparties to derivative contracts to apply risk-mitigation techniques, including timely confirmation and portfolio reconciliation, which function as an operational counterpart to substantive risk and exposure limits.

Sound counterparty and concentration risk management is also a matter of prudent commercial practice and is expected by financing banks, insurers, and trading partners as a condition of extending credit lines, letters of credit, or guarantees to the Company.

Implementation Procedures

6.1 The Compliance/Risk function will maintain a Risk Limits Schedule specifying, for each commodity class, maximum permitted net open position (by volume and notional value), maximum single-counterparty exposure, maximum exposure to any single country or region, and maximum tenor of open positions, reviewed at least annually and approved by the Managing Director.

6.2 Where the Company trades commodity derivatives subject to regulatory position limits set by the Central Bank of Ireland, ESMA, or a trading venue, the Compliance Officer will confirm the applicable limit before trading begins and will monitor live positions against that limit, not solely against the Company's internal risk appetite.

6.3 Counterparty credit risk will be assessed prior to onboarding and reassessed periodically, incorporating counterparty financial standing, payment history, country risk, and (for physical trades) delivery and

performance risk, with exposure aggregated across all open transactions with a given counterparty and its known affiliates.

6.4 Positions and exposures will be reported to the Managing Director at a frequency proportionate to risk (at minimum monthly, and immediately upon a limit breach), with any breach requiring a documented remediation plan and, where a regulatory limit is breached, consideration of whether external notification to the Central Bank of Ireland or the relevant venue is required.

6.5 Concentration risk will be assessed not only by counterparty but by commodity type, geography, and single point of physical logistics failure (for example, reliance on a single port, vessel, or storage facility), consistent with the Company's broader operational risk management expertise.

Responsible Parties: Compliance/Risk Officer (limit setting recommendation and monitoring); Managing Director (final approval of risk appetite and limits); Trading Staff (day-to-day adherence and escalation of near-breaches).

7. Client and Counterparty Onboarding and Due Diligence

Policy Statement

No commodity trading relationship — whether with a client, supplier, buyer, financing institution, or intermediary — will be established or transacted with until that counterparty has been identified, verified, risk-classified, and approved in accordance with this Section, and due diligence will be refreshed periodically and upon trigger events.

The Company will apply due diligence proportionate to risk, applying Simplified Due Diligence only where the CJA 2010 permits it and the risk assessment supports it, standard Customer Due Diligence (CDD) as the default, and Enhanced Due Diligence (EDD) for higher-risk counterparties, transactions, or jurisdictions.

Regulatory Rationale

The CJA 2010 requires Designated Persons to identify and verify customers and beneficial owners before establishing a business relationship or carrying out an occasional transaction above the relevant threshold, to understand the purpose and intended nature of the relationship, and to apply enhanced measures for higher-risk situations, including politically exposed persons (PEPs), high-risk third countries, and complex or unusually large transactions with no apparent economic or lawful purpose.

Where a counterparty relationship falls within MiFID II scope, additional client categorisation obligations apply (see Section 7.4), including appropriateness or suitability assessments depending on the service provided.

Beneficial ownership verification obligations (Section 3) are integrated into the onboarding process rather than treated as a separate step.

Implementation Procedures

7.1 Onboarding will collect and verify, at minimum: full legal identity and registration details of the counterparty; identity and verification of beneficial owners and controlling persons; the counterparty's business activity and rationale for the proposed trading relationship; source of funds and, for higher-risk relationships, source of wealth; and sanctions and PEP screening results.

7.2 Counterparties will be risk-classified (low / standard / high) at onboarding based on factors including jurisdiction, commodity type, transaction structure, use of intermediaries, and PEP or sanctions-adjacent indicators, with the classification driving the applicable due diligence level and ongoing monitoring frequency.

- 7.3 Enhanced** Due Diligence will be applied, at minimum, to counterparties based or beneficially owned in high-risk third countries identified by the European Commission or FATF, PEPs and their close associates and family members, counterparties using complex ownership structures without clear commercial rationale, and transactions involving unusually large volumes of precious metals or cash-intensive settlement.
- 7.4 For** any activity falling within MiFID II scope, clients will be categorised as retail, professional, or eligible counterparty in accordance with MiFID II criteria, with the categorisation documented, communicated to the client, and used to determine the applicable conduct-of-business protections (including appropriateness assessments for non-advised execution).
- 7.5 Onboarding** files will be approved by the Compliance Officer (or, for high-risk relationships, by the Compliance Officer with Managing Director sign-off) before the first transaction is executed, and no trading desk may bypass onboarding approval, including for urgent or time-pressured transactions.
- 7.6 Ongoing** due diligence will be refreshed on a risk-based schedule (at minimum annually for high-risk counterparties, and every two to three years for standard-risk counterparties), and immediately upon a trigger event such as a change in beneficial ownership, an adverse media alert, or a sanctions list update.

Responsible Parties: Compliance Officer (onboarding approval, risk classification, EDD decisions); Business Development / Trading Staff (initial information gathering and relationship management); Managing Director (approval of high-risk relationships).

8. Record-Keeping and Documentation

Policy Statement

Andro Secure will create and retain complete, accurate, and readily retrievable records of all commodity trading activity, client and counterparty due diligence, communications relevant to trading decisions, and compliance monitoring activity, for the retention periods set out in this Section, and will be able to reconstruct any transaction from onboarding through to settlement upon request by an auditor, regulator, or the Company's own compliance function.

Regulatory Rationale

The CJA 2010 requires Designated Persons to retain customer due diligence records and transaction records for five years from the end of the business relationship or the date of the transaction, extendable on request of a competent authority.

MiFID II and MiFIR impose record-keeping obligations on firms providing investment services, including order and transaction records and, for relevant communications, recording of telephone conversations and electronic communications intended to result in a transaction, generally retained for a minimum of five years (and up to seven years on regulatory request).

EMIR requires records of derivative contracts and their modifications to be kept for at least five years following termination of the contract.

Irish company law (the Companies Act 2014, as amended) separately requires the Company to keep adequate accounting records, and general commercial and tax law impose their own retention requirements relevant to trade documentation such as invoices, bills of lading, and letters of credit.

Implementation Procedures

- 8.1 The** Company will maintain a Record Retention Schedule (Appendix C) specifying, for each record category (CDD/KYC files, transaction and trade documentation, derivative contract records, trading communications, sanctions screening results, STRs/STORs, and risk and position reports), the retention period, storage location, and responsible owner, with a minimum default retention of five years unless a longer period applies under this Section or under Irish company law.
- 8.2 Trading** communications relevant to the negotiation and execution of transactions (including calls, emails, and messaging platforms used for business purposes) will be captured and retained; use of personal, unrecorded communication channels for trade-relevant discussions is prohibited.
- 8.3 Records** will be stored securely, with access controls proportionate to sensitivity, back-up arrangements to prevent data loss, and a documented process for producing records to regulators or auditors within the timeframes such requests typically require.
- 8.4 The** Compliance Officer will conduct periodic sampling of transaction files to confirm records are complete and consistent with this Policy, with findings reported as part of the compliance monitoring programme (Section 9).
- 8.5 Records** will not be destroyed before the expiry of the applicable retention period, including where a business relationship has ended, a transaction has settled, or a matter has been closed; legal hold procedures will override standard retention periods where litigation, investigation, or regulatory inquiry is reasonably anticipated.

Responsible Parties: Compliance Officer (retention schedule ownership and file sampling); All Staff (accurate and timely record creation); IT/Operations (secure storage, back-up, and retrieval systems).

9. Conflicts of Interest

Policy Statement

Andro Secure will identify, record, and manage actual and potential conflicts of interest arising from its commodity trading activity, including conflicts between the Company and a client or counterparty, between the Company's trading activity and its other business lines (including physical and maritime security services), and between the personal interests of directors, officers, or employees and the interests of the Company or its counterparties.

Where a conflict cannot be managed to a level that protects the interests of the affected counterparty, the Company will disclose the conflict clearly before proceeding or decline to proceed with the transaction or relationship.

Regulatory Rationale

MiFID II requires firms providing investment services to take all appropriate steps to identify and prevent or manage conflicts of interest, to maintain a conflicts of interest policy, and, where organisational arrangements are not sufficient to manage a conflict, to disclose it to the client before undertaking business.

Directors' general fiduciary duties under Irish company law, including the duty to avoid conflicts of interest and to act in good faith in the interests of the Company, apply independently of MiFID II and are relevant given the Managing Director's dual role as founder, senior operator, and decision-maker across multiple Andro Secure business lines and commercial ventures.

Conflicts arising from group or affiliate structures (including cross-referrals between the Company's security and trading businesses, or between trading and any commodity financing arrangements the Company or its principals

are involved in) require particular attention because they are less visible to external counterparties than conflicts with unrelated third parties.

Implementation Procedures

- 9.1 The** Compliance Officer will maintain a Conflicts of Interest Register recording identified actual and potential conflicts, the nature of the conflict, the management or mitigation steps taken, and, where applicable, the disclosure made to the affected party.
- 9.2 Before** onboarding a new counterparty or agreeing a new transaction structure, trading staff will consider and document whether the Company, an affiliate, or any director or employee has an undisclosed interest in the counterparty, the transaction, or a competing transaction, escalating any such interest to the Compliance Officer before proceeding.
- 9.3 Personal** dealing, outside business interests, and gifts and hospitality relevant to trading relationships will be subject to prior disclosure and, where appropriate, approval, under the Company's personal account dealing and gifts and hospitality procedures (Appendix D).
- 9.4 Where** the Managing Director or another senior decision-maker has a personal or related-party interest in a proposed transaction or counterparty, that individual will be excluded from the approval decision, which will instead be taken by the Compliance Officer together with an independent member of senior management or external adviser.
- 9.5 The** Conflicts of Interest Register will be reviewed at least annually by the Compliance Officer and reported to the Managing Director, with material or recurring conflicts flagged for structural remediation rather than repeated case-by-case management.

Responsible Parties: Compliance Officer (register maintenance and disclosure decisions); Directors and Employees (proactive disclosure of personal and related-party interests); Managing Director (structural remediation of recurring conflicts, subject to recusal where personally conflicted).

10. Compliance Monitoring, Breach Detection, and Regulatory Reporting

Policy Statement

Andro Secure will operate an ongoing compliance monitoring programme covering AML/CFT, sanctions, market conduct, position and risk limits, onboarding quality, and record-keeping, designed to detect breaches of this Policy and of applicable law promptly, and will escalate and, where legally required, report breaches to the appropriate regulator without undue delay.

All staff have a personal obligation to report suspected breaches of this Policy or of applicable law, through the escalation channels set out in this Section, without fear of retaliation.

Regulatory Rationale

Effective ongoing monitoring is an express expectation under the CJA 2010 (as part of a Designated Person's AML/CFT programme) and is treated by the Central Bank of Ireland as a core element of good governance for regulated and AML-obliged entities, reflected in Central Bank guidance on fitness and probity and on effective compliance functions.



Firms within MiFID II scope are required to maintain a permanent and effective compliance function, and Andro Secure applies an equivalent standard voluntarily across all of its commodity trading activity irrespective of authorisation status.

Certain breaches — including confirmed sanctions breaches, suspected money laundering, and suspected market abuse — carry independent statutory reporting obligations to specific authorities (the Central Bank of Ireland, FIU Ireland, the Department of Foreign Affairs, or ESMA/the relevant venue, as applicable) that operate alongside, and are not satisfied merely by, internal escalation.

Implementation Procedures

- 10.1 The** Compliance Officer will maintain an annual Compliance Monitoring Plan covering, at minimum: sanctions and AML screening quality assurance, onboarding file sampling, position and risk limit adherence, trading communications surveillance, and record-keeping completeness, with findings documented in a monitoring log.
- 10.2 The** Company will maintain a clear internal escalation channel (in the first instance, to the Compliance Officer, and, for matters involving the Compliance Officer, directly to the Managing Director or, where appropriate, to external legal counsel) for staff to report suspected breaches, policy violations, or misconduct, including on a confidential or anonymous basis.
- 10.3 Every** reported or detected breach will be logged in a Breach Register recording the nature of the breach, root cause, affected transactions or counterparties, remediation actions, and whether external notification was required, with the register reviewed by the Managing Director at least quarterly.
- 10.4 Where** a breach triggers a statutory reporting obligation (including a Suspicious Transaction Report to FIU Ireland, a Suspicious Transaction and Order Report to the Central Bank of Ireland, a sanctions breach notification, or a material prudential or conduct issue reportable to the Central Bank of Ireland), the report will be made within the applicable statutory timeframe, and in any event without undue delay, by the Compliance Officer or MLRO.
- 10.5 The** Compliance Officer will provide a written Compliance Report to the Managing Director at least quarterly, summarising monitoring results, breaches identified, regulatory reports made, and the status of remediation actions, and will report immediately, outside the normal cycle, on any material or urgent matter.
- 10.6 No** staff member will face retaliation for a good-faith report of a suspected breach; any such retaliation will itself be treated as a disciplinary matter under Section 12.

Responsible Parties: Compliance Officer / MLRO (monitoring programme, breach register, statutory reporting); All Staff (first line reporting obligation); Managing Director (quarterly review and resourcing of the compliance function).



11. Training, Competence, and Certification

Policy Statement

Andro Secure will ensure that all directors, officers, and employees involved in commodity trading, onboarding, or compliance activity receive training appropriate to their role, before undertaking relevant duties and on a recurring basis thereafter, and will maintain records evidencing that training.

Regulatory Rationale

The CJA 2010 requires Designated Persons to provide staff with AML/CFT training enabling them to recognise transactions linked to money laundering or terrorist financing and to know the procedures to follow.

The Central Bank of Ireland's fitness and probity regime, and MiFID II's organisational requirements for firms with authorised activity, both reflect a broader regulatory expectation that individuals performing controlled or trading-related functions maintain an appropriate and current level of competence.

Given the specialised nature of precious metals, energy, and agricultural commodity trading, general AML and market conduct training is supplemented with commodity- and product-specific training to ensure staff can recognise sector-specific red flags (for example, in trade finance instruments or physical logistics documentation).

Implementation Procedures

- 11.1 New** joiners with trading, onboarding, or compliance responsibilities will complete induction training covering this Policy, AML/CFT and sanctions procedures, market abuse prohibitions, and record-keeping requirements, before independently handling client or counterparty relationships or executing transactions.
- 11.2 All** relevant staff will complete refresher training at least annually, updated to reflect regulatory developments, findings from the Company's own compliance monitoring, and any incidents or near-misses identified during the year.
- 11.3 Training** will be role-tailored: trading staff will receive additional focus on market abuse, position limits, and product-specific red flags; onboarding staff will receive additional focus on CDD/EDD standards and beneficial ownership verification; and senior management will receive training on governance, conflicts of interest, and their oversight responsibilities.
- 11.4 The** Compliance Officer will maintain training records for each individual, including course content, date completed, and any assessment result, retained for the duration of employment and for the record-retention period applicable under Section 8 thereafter.
- 11.5 Where** an individual does not complete required training within the applicable timeframe, or fails a competence assessment, that individual will not perform the relevant duties independently until remediated, with the matter escalated to the Managing Director.

Responsible Parties: Compliance Officer (training design, delivery, and record-keeping); Managing Director (resourcing and prioritisation of training); All Staff (completion of required training within set timeframes).



12. Enforcement, Disciplinary Procedures, and Remediation

Policy Statement

Compliance with this Policy is a condition of employment or engagement for all directors, officers, employees, contractors, and agents of Andro Secure Group Ltd involved in commodity trading activity. Breaches will be addressed proportionately, consistently, and promptly, ranging from coaching and additional training for inadvertent, low-impact breaches, through to disciplinary action up to and including termination, and referral to regulators or law enforcement, for serious, deliberate, or repeated breaches.

Regulatory Rationale

Failure to comply with AML/CFT, sanctions, and market abuse obligations can expose both the individual and the Company to criminal liability, civil penalties, and regulatory sanction under the CJA 2010, EU sanctions law, MAR, and MiFID II, in addition to reputational and counterparty-relationship harm; a proportionate and consistently applied internal disciplinary framework is both good governance and a mitigating factor regulators typically take into account when assessing corporate culture and control failures.

Irish employment law requires disciplinary processes to be fair and consistent with the Company's own procedures and with the Workplace Relations Commission's Code of Practice on Grievance and Disciplinary Procedures; this Policy's enforcement provisions operate alongside, and do not replace, the Company's general HR disciplinary policy.

Implementation Procedures

- 12.1 Any** confirmed breach of this Policy will be assessed by the Compliance Officer (or, where the Compliance Officer is implicated, by the Managing Director together with external legal counsel) for severity, intent, and impact, using a documented severity matrix (minor / moderate / serious / severe) set out in Appendix E.
- 12.2 Minor**, inadvertent breaches with no client, counterparty, or regulatory impact will typically be addressed through coaching, additional supervision, and targeted retraining, recorded on the individual's compliance file.
- 12.3 Moderate** or repeated breaches, or breaches involving a failure to escalate known issues, will be addressed through formal disciplinary process under the Company's HR procedures, which may include a formal warning, restriction of trading authority, or reassignment of duties.
- 12.4 Serious** or severe breaches — including deliberate circumvention of sanctions screening, concealment of a conflict of interest, participation in or facilitation of market manipulation, or failure to report known suspicious activity — will be treated as gross misconduct, may result in summary termination, and will be assessed for mandatory external reporting to the Central Bank of Ireland, FIU Ireland, An Garda Síochána, or other relevant authority.
- 12.5 Where** a breach has caused, or risked causing, financial or other harm to a client, counterparty, or third party, the Compliance Officer will coordinate a remediation plan, which may include client or counterparty notification, financial redress, and enhanced monitoring of the affected relationship or business area.
- 12.6 Root-cause** analysis will be conducted for every serious or severe breach, and, where the root cause reflects a gap in this Policy or in the Company's control environment rather than solely individual conduct, the Compliance Officer will propose a corresponding Policy or control amendment under Section 13.

Responsible Parties: Compliance Officer (breach assessment and remediation coordination); Managing Director / HR (disciplinary decision-making); External Legal Counsel (advice on external reporting obligations and legal exposure).



13. Policy Governance, Review, and Amendment

Policy Statement

This Policy is owned by the Compliance Officer and approved by the Managing Director. It will be formally reviewed at least annually, and earlier were triggered by material regulatory change, a material change in the Company's commodity trading activities, or a significant compliance finding or breach.

Implementation Procedures

- 13.1 The** Compliance Officer will maintain the version control log at the front of this document, recording every substantive amendment, its rationale, its author, and its approval date.
- 13.2 Any** amendment to this Policy will be approved by the Managing Director before it takes effect, save for minor administrative or formatting corrections, which the Compliance Officer may make directly and log accordingly.
- 13.3 Following** any material amendment, the Compliance Officer will ensure affected staff are briefed on the change and, where necessary, receive supplementary training, before the amended provisions take effect operationally.
- 13.4 This** Policy will be made available to relevant regulators, external auditors, and, on reasonable request and subject to appropriate confidentiality protections, to trading counterparties conducting their own due diligence on Andro Secure.

Responsible Parties: Compliance Officer (ownership, review cycle, version control); Managing Director (approval authority).



Appendices

The following appendices are referenced throughout this Policy and are maintained as separate controlled documents, attached or available on request from the Compliance Officer. They are listed here for completeness and to identify where operational detail supporting each Policy section is held.

Ref.	Title	Purpose / Cross-Reference
Appendix A	Regulatory Perimeter Assessment Template	Used under Section 2 to classify new commodities, products, or activities against MiFID II / EMIR scope and available exemptions.
Appendix B	Sanctions and AML Screening Procedure	Detailed screening workflow, escalation matrix, and STR filing procedure referenced under Section 3.
Appendix C	Record Retention Schedule	Full record category, retention period, and storage location matrix referenced under Section 8.
Appendix D	Personal Account Dealing and Gifts & Hospitality Procedure	Referenced under Section 9 for disclosure and approval of personal trading and gifts/hospitality.
Appendix E	Breach Severity Matrix and Disciplinary Guidelines	Referenced under Section 12 for consistent assessment of breach severity and disciplinary outcome.
Appendix F	Client and Counterparty Onboarding Checklist (KYC/CDD/EDD)	Referenced under Section 7; includes standard and enhanced due diligence document checklists by counterparty type.
Appendix G	Risk Limits Schedule	Referenced under Section 6; sets out current position, counterparty, and concentration limits by commodity class.
Appendix H	Regulatory Contacts and Escalation Directory	Central Bank of Ireland, FIU Ireland, ESMA, and other relevant regulator contact points and notification procedures.

End of Policy.

