IGUAKO CAPITAL · Group policy

Market Abuse Prevention

This policy sets out how IGUAKO Capital prevents, detects and reports conduct that would constitute market abuse: dealing on inside information, unlawful disclosure, and manipulation of a price, an order book or a benchmark. It requires surveillance of every order, trade and recorded communication across the eleven trading and execution desks, the review of every alert within two business days, and the reporting of suspicious conduct to the relevant authority. It applies to all six divisions and to every member of staff, wherever the conduct occurs.

CODE	CATEGORY	VERSION
IGC-MT-001	Markets and trading	3.3
EFFECTIVE	**REVIEW**	**OWNER**
2022-04-01	Annual; last reviewed April 2026, next review due April 2027	Head of Surveillance and Market Conduct

1. Purpose and scope

The firm trades for its proprietary balance sheet of US$610 million, for managed accounts and for clients across listed and over-the-counter markets, and it holds inside information in the course of its Investment Banking, Private Equity and Commercial Finance work. This policy exists to ensure that neither the firm nor any person in it uses that position to abuse a market, and that the firm can demonstrate as much to any authority that asks.

The policy applies to every financial instrument in which the firm or its clients deal, to every order whether executed or not, to every trading desk and to every person with access to trading systems or to inside information. It applies to conduct wherever it occurs, including outside working hours and on personal accounts, and to conduct by a third party that a member of staff becomes aware of.

The Information Barriers and Inside Information policy governs how inside information is contained; the Personal Account Dealing policy governs staff trading; the Order Handling and Allocation policy governs the sequence and allocation of orders. This policy governs the abusive conduct itself and the surveillance that detects it.

2. Definitions

Inside information is information of a precise nature that has not been made public, relating to an issuer or an instrument, which a reasonable investor would be likely to use as part of the basis of an investment decision. Insider dealing is dealing, or attempting to deal, on the basis of inside information, or recommending or inducing another person to do so. Unlawful disclosure is the disclosure of inside information other than in the normal exercise of employment.

Manipulation is any transaction, order or behaviour that gives or is likely to give a false or misleading signal as to the supply, demand or price of an instrument, that secures a price at an artificial level, or that employs a deceptive device or contrivance. It includes placing orders with no intention of executing them, trading at the close to influence a reference price, and disseminating information the person knows to be false.

An alert is an automated or manual flag raised by the surveillance system or by a person against a pattern set out in the surveillance rulebook. A level 2 review is an escalated review of an alert by the Head of Surveillance and Market Conduct with the desk head excluded. A suspicious activity report is the firm's report of conduct it reasonably suspects to constitute market abuse, made to the relevant authority in the jurisdiction concerned.

3. Principles

The firm does not deal, and does not permit any person to deal, on inside information, whatever the source and whatever the expected gain. The firm does not disclose inside information except where the disclosure is necessary to its work and the recipient has been made an insider under the Information Barriers policy. The firm does not place an order it does not intend to execute.

Surveillance is independent of the desks it monitors. The surveillance function reports to the General Counsel and Group Head of Compliance and not to any divisional head. Desk heads see the alerts raised on their desks after the surveillance function has reviewed them, not before, and cannot close an alert themselves.

The firm reports suspicion, not proof. Where the surveillance function reasonably suspects abuse after a level 2 review, the report is made whether the person concerned is a member of staff, a client or a counterparty, and the person is not told that a report has been made.

4. Requirements

Every order and every execution across the eleven desks in George Town, New York, London, Zürich, Singapore, Hong Kong and Sydney is captured in the surveillance system on the day of the event with its timestamp, the instrument, the account, the trader, the venue or counterparty and the price. The rulebook holds 34 automated patterns covering insider dealing, front running, layering, spoofing, wash trades, marking the close, reference-price influence and cross-desk coordination, each with a calibrated threshold approved by the Head of Surveillance and Market Conduct.

All business communication on recorded channels, including voice lines on the desks, electronic messaging and email, is captured and subject to lexicon and pattern surveillance. Business communication on an unrecorded channel, including a personal device or a consumer messaging application, is prohibited. A member of staff who receives a business message on such a channel copies it to a recorded channel the same day and does not reply on the original.

Each alert is reviewed by a surveillance analyst within two business days of generation. An alert closed as a false positive is recorded with the reason. An alert not closed at first review is escalated to level 2 within a further three business days. A level 2 review that finds reasonable suspicion results in a suspicious activity report within five business days of that finding. The surveillance system checks every order against the restricted list, the watch list and every open insider list before and after execution.

Every member of staff completes market abuse training on joining and annually thereafter, and passes an assessment. Traders and persons with access to inside information complete an additional module on the patterns in the rulebook. Every member of staff attests annually that they have read this policy and that they have not dealt, disclosed or recommended on the basis of inside information.

- All orders, executions and recorded communications captured on the day of the event.

- 34 automated patterns in the rulebook, with thresholds approved by the policy owner.
- Alert review within two business days; level 2 escalation within a further three.
- Suspicious activity report within five business days of a level 2 finding.
- Pre-trade and post-trade check of every order against the restricted, watch and insider lists.
- No business communication on unrecorded channels.
- Annual training, assessment and attestation for every member of staff.

5. Roles and responsibilities

The Head of Surveillance and Market Conduct owns this policy, the rulebook and the surveillance system, decides level 2 reviews, approves suspicious activity reports jointly with the General Counsel and Group Head of Compliance, and reports quarterly to the Compliance & Conduct Committee. The surveillance team of six analysts sits in London and Singapore and covers every trading hour of the eleven desks.

Desk heads are accountable for the conduct of their desks, for ensuring that every order has a documented rationale where the rulebook requires one, and for supporting surveillance reviews within two business days of a request. The Group Head of Trading and Execution is accountable for the completeness of order capture. The Head of the Control Room maintains the lists the surveillance system relies on.

Every member of staff who suspects market abuse, by anyone, reports it to the surveillance function or through whistleblowing@iguako.tech the same day. Reporting a suspicion in good faith is protected under the Whistleblowing and Speaking Up policy, and the identity of the person reporting is not disclosed to the desk concerned.

6. Monitoring and reporting

The surveillance function reports monthly to the General Counsel and quarterly to the Compliance & Conduct Committee on alerts generated, closed and escalated by pattern and desk, the time taken at each stage against the standard, suspicious activity reports made, rulebook changes and training completion. The rulebook thresholds are recalibrated every six months against the alert outcomes, and every recalibration is documented and approved.

In the twelve months to 30 June 2026 the system generated 1,412 trade alerts, of which 1,371 were closed at first review as false positives or explained, 41 went to level 2, and four resulted in suspicious activity reports. Three of the four concerned counterparty or client conduct and one concerned a member of staff, who left the firm. The median time from alert to first review was one business day.

Communication surveillance produced 218 lexicon alerts in the same period, of which 11 went to level 2 and none resulted in a report. Internal Audit reviews the surveillance system, the rulebook and a sample of closed alerts every year, and an external specialist reviews the rulebook every three years.

7. Breaches

A breach of this policy is any dealing, disclosure or recommendation on inside information, any manipulative order or transaction, any business communication on an unrecorded channel, any order not captured in the surveillance system, any alert not reviewed within the standard, and any suspicion known to a member of staff and not reported. A breach is recorded on the day of discovery.

Conduct amounting to market abuse by a member of staff results in dismissal and is reported to the relevant authority. The firm cooperates with any subsequent investigation and does not settle with the person in a way that would prevent that cooperation. Where a client or counterparty is found to have abused a market through the firm, the relationship is ended and the report is made.

Lesser breaches, such as a message on an unrecorded channel or a late alert review, are recorded in the compliance breach log and addressed under the Code of Conduct. Fourteen unrecorded-channel breaches were recorded in the year to 30 June 2026, all self-reported, and each resulted in retraining; two second occurrences resulted in written warnings.

8. Review

The Head of Surveillance and Market Conduct reviews this policy annually, the rulebook every six months and the surveillance system's coverage whenever a desk, an instrument class or a venue is added. The review is approved by the Compliance & Conduct Committee, and the Board is told of any change to the reporting standard.

The policy was first issued in April 2022 when the New York desk began trading. Version 3.3, approved in April 2026, added the cross-desk coordination patterns and the six-monthly recalibration of thresholds. The next review is due in April 2027.

Key controls

- Independent surveillance function reporting to the General Counsel, not to any desk.
- Complete same-day capture of orders, executions and recorded communications.
- Rulebook of 34 patterns with documented thresholds recalibrated every six months.
- Two-business-day alert review, three-business-day level 2 escalation and five-business-day reporting.
- Automated pre-trade and post-trade screening against the restricted, watch and insider lists.
- Recorded-channel rule with same-day copy of any business message received elsewhere.
- Annual training, assessment and attestation for all 312 staff.
- Annual Internal Audit review and three-yearly external rulebook review.

Related policies

- Information Barriers and Inside Information (IGC-MT-004)
- Personal Account Dealing (IGC-MT-003)
- Order Handling and Allocation (IGC-MT-006)
- Whistleblowing and Speaking Up (IGC-GR-004)

Colophon

IGUAKO Capital is a work of institutional fiction by the Iguako Institute for Applied Unreality (iguako.tech). This document is part of that work. It creates no rights or obligations, describes no licensed entity and is not an offer, a contract, a client record or advice.