GROUP POLICY

Chow Tai Fook Jewellery Group Limited

Group Anti-Money Laundering and Sanctions Compliance Policy

Policy Version
V2

Policy Function
Group Risk Management Department

Policy Approver
Group MLRO

1. PURPOSE

1.1 Our Commitment

Chow Tai Fook Jewellery Group Limited (the "Company") and its subsidiaries (collectively, the "Group") acknowledge the importance of preventing and combating money laundering, terrorist financing, arms proliferation financing, and sanctions violations (in this Policy, collectively "financial crime" unless the context otherwise requires) and its critical relevance to us as a leading global jewellery brand dealing with precious metal and stones. The Group is committed to complying with all applicable laws and regulations against financial crime across all jurisdictions where it operates.

1.2 Safeguard Brand Integrity and Minimize Associated Risks

To safeguard the integrity of the Group's brand and minimize the risks associated with the heightened legal obligations in the jewellery industry in the major business markets of the Group (each a "Business Market"), the Group revised its original Anti-money Laundering Policy and introduced this Group Anti-Money Laundering and Sanctions Compliance Policy ("Policy") in 2025. This Policy is supplemented by the policies, guidelines and standard operating procedures issued by Business Markets to provide practical guidance on the key control measures to our management and staff (in this Policy, "staff" shall include both employees and non-employment individuals of the Group, such as the employees of franchisees of the Group).

1.3 Financial Crime Governance Framework

In line with the international standards of combating financial crime, as well as the specific legal and regulatory requirements under the Dealers in Precious Metals and Stones ("DPMS") registration regime in Hong Kong and other corresponding regimes in which each of our Business Markets operates (collectively "applicable requirements" unless the context otherwise requires), the Group has established an overarching governance framework underlying this Policy ("Group Financial Crime Governance Framework "). It provides a consistent approach and fundamental principles for financial crime compliance by all its subsidiaries and branches globally while allowing for necessary adaptions by Business Markets based on their local legal obligations and market contexts, provided that such adaptation shall not compromise the integrity of the Group Financial Crime Governance Framework. For the avoidance of doubt, while each Business Market must comply with their local legal financial crime regulations, the subsidiaries of the Group should also ensure compliance with the Hong Kong DPMS regime.

2. SCOPE

This Policy applies to all directors and staff of the Group and the franchisees of the Group.

3. AUTHORISATION, OVERSIGHT AND OVERALL GOVERNANCE

3.1 Group Financial Crime Governance Structure

Director, Risk Management is authorised by and accountable to the Board to serve as the Group Money Laundering Responsible Officer ("Group MLRO"), who is responsible for establishing, leading and overseeing the Group's Financial Crime Governance Framework. To accommodate jurisdictional differences, each Business Market Head together with the Market Money Laundering Responsible Officer ("Market MLRO") are vested with the power and responsibility to implement, adapt and coordinate the Group Financial Crime Governance Framework within their Business Market, with the support of a market-level Anti-Money Laundering Taskforce ("Market AML Taskforce") that consists of the necessary expertise, resources and influence.

3.2 Management Oversight

Senior management of Group functions and Business Market Heads are responsible for overseeing the implementation of compliance measures to manage the financial crime risks within their respective areas and across the Group. Group MLRO and Market MLROs should report identified financial crime issues at management meetings, as and when necessary and in a timely, complete, understandable and accurate manner, to ensure that the Board/Board Committees, the Group MLRO, Business Market Heads, C-Suite Officers and other senior management (where applicable) are provided with the necessary information to make informed decisions.

3.3 Policy Review and Revision

The Group MLRO is vested with the power and responsibility to review and update this Policy as and when needed to reflect changes in laws and regulations as well as in the Group's compliance controls. Review and updates should be carried out at least on an annual basis to ensure the Group Financial Crime Governance Framework and associated measures remain effective in light of evolving laws and regulations, business operations and business environment.

3.4 Market SOPs and Discrepancy Resolution

Business Market Heads, with the support of Market MLROs and Market AML Taskforces, are authorised to adapt and translate this Policy into market-level policies, guidelines and standard operating procedures (collectively, "Market SOPs"). Such adaptation must align with local laws and regulations on financial crime without compromising the Group Financial Crime Governance Framework. Market SOPs should be reviewed at least annually for updates and submitted to the Group MLRO and the Group Legal Department for endorsement and incorporation. Any major discrepancies with this Policy must be escalated by Market MLROs to the Group MLRO and the Group Legal Department for resolution and guidance.

4. RISK ASSESSMENTS

Under the applicable requirements, the Group must conduct comprehensive risk assessment of its financial crime compliance regularly and prior to taking any actions that could impact the business and risk profile of the Group as a whole. The assessment shall enable the Group to understand its exposure to financial crime, and shall include an evaluation of whether the existing controls are capable of managing the identified risks and documenting the measures needed to address newly identified risks or related matters. The relevant risk assessment should be initiated by the Group Function Head or Business Market Head prior to taking actions that changes the Group's risk profile, or at least conducted along with the risk management cycle of the Group as may be set out in the risk management policy and/or guidance documents issued by associated Group function(s).

5. INTERNAL CONTROLS

This section sets out the key aspects of the Group's internal controls against financial crime, to ensure that a consistent approach is adopted throughout the Group and that each Business Market is in compliance with the applicable requirements.

5.1 Legal Requirements Specific to Payment Methods and Transaction Value

Under applicable requirements on financial crime compliance, the Group is required to establish control measures specific to (i) certain payment methods used to transact with customers and counterparties and (ii) transactions with value crossing specified thresholds, which are subject to change from time to time.

5.2 Know Your Customers/Counterparties and Due Diligence Requirements

5.2.1 **Customer / counterparty due diligence ("CDD"):** The Group is required under applicable requirements to perform CDD, particularly when it is involved in dealings in precious metals and stones. As a matter of policy, the Group also requires CDD to be undertaken in relation to procurement transactions (such as the transaction exceeding a specific value threshold). Performing CDD enables the Group to understand its customers and counterparties as well as to implement appropriate measures to reduce the risk of the Group involving in money laundering, terrorist financing or arms proliferation financing related activities and/or breaching sanctions laws and regulations. The Group adopts a risk-based approach to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

1) In respect of retail customers, frontline staff must perform CDD:
    a. before carrying out a transaction that exceeds the specified threshold;
    b. when there are doubts about the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity; or
    c. when there are other factors rendering the customer or transaction suspicious.

2) In respect of counterparties, back-office staff must perform CDD:
   a. before carrying out a transaction that exceeds the specified threshold;
   b. when the counterparty is incorporated or operates in any high risk countries or jurisdictions;
   c. when the counterparty sources raw materials/finished products from high risk countries or jurisdictions;
   d. when there are doubts about the veracity or adequacy of any information previously obtained for the purpose of identifying the counterparty or verifying the counterparty's identity; or
   e. when there are other factors rendering the counterparty or transaction suspicious.

Market SOPs should provide more guidance on CDD and further reference on the applicable threshold for high value transaction, high risk countries and jurisdictions and factors that may be relevant to the identification of suspicious transactions.

5.2.2 **Enhanced due diligence ("EDD"):** Frontline and back-office staff must apply EDD measures in relation to a business relationship or transaction that presents a high risk of money laundering, terrorist financing, arms proliferation financing or sanctions violations (either as identified by the Group or as specified by a written notice from a government or regulatory authority), which would require additional measures to identify and verify relevant information (such as the customers' or counterparties' identity and source of funds) and perform additional ongoing CDD. Market SOPs should provide more guidance on EDD.

5.2.3 **Ongoing CDD:** After establishing a business relationship, ongoing CDD must be performed on the customers' or counterparties' profiles to monitor their status and activities, and relevant records must be properly maintained. Additional review must be performed (i) when there is a change in beneficial ownership and/or control of the customers/counterparties or (ii) upon reactivation of the relationship with a dormant customer/counterparty. Market SOPs should provide more guidance on ongoing CDD.

5.3 Suspicious Transaction Reporting

5.3.1 The Group is required by applicable requirements to monitor transaction for suspicious activities and report transactions suspected of money laundering, terrorist financing or arms proliferation financing to competent regulatory bodies and enforcement agencies (collectively referred to as "Regulatory Bodies"). The same requirement applies to transactions involving persons subject to applicable sanctions.

5.3.2 In support of this, the Group has developed an internal reporting process to ensure proper and timely reporting of suspicious transactions for further review and decision. When there is suspicion or knowledge of money laundering, terrorist financing, arms proliferation financing or sanctions violations, the responsible staff must file an internal Suspicious Transaction Report ("STR") to the Group MLRO, the respective Market MLRO and AML Taskforce, as soon as possible and without undue delay. Upon receipt of an internal STR, Market MLRO must promptly work with the members of Market AML Taskforce along with Legal, Finance, Executive Office and any other subject matter expertise and capacities to conduct a preliminary assessment on whether there is a need to file an external STR to the relevant Regulatory Bodies. Market MLRO must then submit the relevant assessment findings and recommendations to Business Market Head, the Group Legal Department and the Group MLRO, who must review and decide whether to file an external STR.

5.3.3 In respect of external reporting, each Market MLRO will act as the central point of contact. If it is decided that external STR is required, the Market MLRO must promptly report the suspicious transaction to the relevant Regulatory Bodies. Market MLROs must establish and maintain a record of all STRs made.

5.3.4 Upon receiving the above assessment, Business Market Head, supported by the Group MLRO and the Group Legal Department, shall determine whether it is necessary to terminate the relevant transaction or business relationship. The Business Market Head may authorise their direct delegates to act on his/her behalf, provided the delegates are authorised in writing to make such decisions.

5.3.5 Market SOPs should provide more guidance on suspicious transaction reporting.

5.4 Other Reporting Obligations

5.4.1 In addition to the requirement to report suspicious transactions, the Group must comply with other requirements under applicable local laws to report "high value transactions". Market SOPs should provide more guidance on "high value transaction" reporting requirements.

5.4.2 In all cases, for each Business Market, the Group MLRO and Market MLRO are responsible for assessing whether such reporting is required with the support of Market AML Taskforce, before making reports to the relevant Regulatory Bodies in accordance with local requirements, and maintaining a record of all transactions reported.

5.5 Confidentiality Protection

5.5.1 **Protection of personal data:** The Group and all Group personnel must keep confidential, in accordance with the applicable local data privacy laws, information relating to customers, counterparties and any other person which may have been obtained in the course of the Group's financial crime compliance efforts, subject to any legal requirements to disclose such information in accordance with law, including in making reports to Regulatory Bodies.

5.5.2 **Strict prohibition on tipping off**: The Group and Group personnel must not disclose to any person any information which is likely to prejudice any investigation into any suspicious transaction ("tipping off"), including in circumstances where suspicion has been raised within the Group but has not yet been reported to the Regulatory Bodies. Such actions would otherwise constitute a criminal offence.

5.6 Periodic Transaction Review

5.6.1 Periodic review of transactions enables the Group to identify and detect any anomalies in transactions, potential suspicious activities, trends or patterns, and to take remedial actions promptly. Transaction reviews in respect of customers and counterparties should be carried out on a monthly basis by the Market MLROs. Assessments and analyses performed as part of transaction reviews must be documented in writing and provided to the Group MLRO for review.

5.6.2 All transactions shall be reviewed using a risk-based approach, taking into account the Group's knowledge of the customer/counterparty, and the customer/counterparty's business, risk profile and sources of fund. Transactions that are complex, unusually large in amount or of an unusual pattern, and have no apparent economic or lawful purpose, must be identified for further assessment.

5.7 Independent Audits and Checks

The Group shall conduct regular independent audits or checks of its financial crime compliance systems and measures to continuously ensure and enhance their effectiveness. The frequency and scope of the audits and checks should be commensurate with the nature, scale and complexity of the business of the Group and the Business Market in question, as well as the specific financial crime risks associated with each Business Market. Where appropriate, the Group may arrange such audits or checks to be carried out by the internal audit function, other functions independent of the development and implementation of the system, or alternatively, by qualified third party organisations.

5.8 Staff Training and Awareness Building

5.8.1 Ongoing staff training is an important element to prevent and detect activities related to money laundering, terrorist financing or arms proliferation financing and sanctions violations. The content and frequency of the training shall be tailored to the local legal obligations, market contexts as well as the job functions of the relevant staff.

5.8.2 The Group shall provide regular training to all relevant Group personnel enhance their awareness towards financial crime risks, as well as ensuring that they are capable of implementing necessary internal controls.

5.9 Record Keeping and Information Sharing

5.9.1 The Group recognizes the importance of record keeping to the effective management of financial crime related investigations. Market MLROs are responsible for ensuring all relevant review and compliance records (for example, records of CDD checks, records of transactions and details of action taken in respect of internal and external STR) are maintained properly.

5.9.2 We keep our records in the form of original documents or copies in either hard copy or electronic form. All electronic records are subject to regular and routine backup.

5.9.3 All relevant records must be kept for the duration of a business relationship, and for a minimum of a specified period after its end or the completion of a transaction. The specified period applicable for each of the Business Markets will be provided in Market SOPs , and in any case shall be no less than five years. A longer period may be applied when required by a relevant authority or a Regulatory Body in writing in respect of a specified transaction or customer.

5.9.4 To the extent permitted by the laws and regulations of the jurisdiction of each Business Market, and subject to confidentiality and proper use of the shared information (including the prevention of tipping off), the Group should establish an internal mechanism for information sharing at the Group level. Such mechanism should be designed to support due diligence, manage risks associated with money laundering, terrorist financing, arms proliferation financing and sanctions, and combat related crimes.

5.10 Sanctions Compliance

5.10.1 The Group is committed to identifying and mitigating any risks of sanctions violations and complying with all relevant economic and trade sanctions laws as they apply to the Group's business activities in all relevant jurisdictions.

5.10.2 When establishing new or reactivating relationships with customers, counterparties or staff members, sanctions screening must be performed as part of the CDD and/or EDD process. This involves checking the specific customers, counterparties (including their ultimate beneficial owners) and staff members against the sanctions lists applicable in the relevant jurisdictions (including but not limited to the consolidated list of persons subject to sanctions by the United Nations Security Council) ("Sanctions Database"), or using the sanctions screening tool that the Group has subscribed to (if available) ("Sanctions Screening Tool"), to ensure they are not sanctioned before proceeding with the transaction. Market SOPs should provide guidance on the sanctions list for the relevant jurisdiction.

5.10.3 As sanctions lists are updated regularly, after the establishment of the business relationships, the relevant customers, counterparties (including their ultimate beneficial owners) and staff members must be screened against the most updated sanctions lists in the Sanctions Database or using the Sanctions Screening Tool (if available) on a regular basis.

5.10.4 If any customer, counterparty or staff member is confirmed to be a sanctioned party, the business or employment relationship should be reviewed for decision as to whether (i) the relationship should be terminated and (ii) an external STR should be filed with the relevant Regulatory Bodies as soon as possible.

6. REPORTING

6.1 Market to Group Reporting

Market MLROs should report the findings of monthly transaction review set out in section 5.6 and a summary of significant money laundering or sanctions related incidents or investigations to the Group MLRO on a monthly basis, or more frequently where necessary. This enables the Group MLRO to fairly assess the financial crime compliance risks of the Group.

6.2 Group-level Reporting

The Group MLRO shall report to the Board, Board Committees and senior management annually/as and when needed, updating them on the assessment of the financial crime compliance risks of the Group. This ensures that the Policy remains relevant and up-to-date and allows for informed feedback on the compliance strategy.

7. WHISTLEBLOWING

For any serious misconduct, fraud or irregularities, whether actual or suspected, in relation to any breach of this Policy, Directors, employees and relevant external parties should report to the Group Whistleblowing via the following channels promptly:

Dedicated Whistleblowing Email box: *wb@chowtaifook.com*;

or by mail with a cover letter with any available evidence in a sealed envelope marked "Strictly Private and Confidential – to be opened by the addressee only", and mail it to:

Attn: Whistleblowing Policy Officer

Address: Chow Tai Fook Jewellery Group Limited

38/F New World Tower , 16-18 Queen's Road Central, Hong Kong

8. LANGUAGE VERSION

In the event of a conflict between multiple language versions, the English version shall prevail.

9. VERSION CONTROL

Version	Key Updates	Policy Owner/Department	Effective Date
V1	First release	Group Policy & Control	17/04/2020
V2	• Revised key principles in line with the updated requirements of applicable legal and regulatory requirements in Hong Kong, Macau, Mainland China and Taiwan • Introduced the financial crime governance framework and corresponding internal controls	Group MLRO	07/04/2025

10. REFERENCE/ SUPPLEMENTARY DOCUMENT

Market SOPs should be developed to provide practical measures and strategies for our management and frontline and back-office staff to uphold the principles laid down in this Policy.

ALL RIGHTS AND CONFIDENTIALITY NOTICE

This document and its materials (collectively referred to as the "Release") are the property of Chow Tai Fook Jewellery Group Limited, its subsidiaries, affiliates, and/or licensors (collectively or individually referred to as the "Company"). The Release is strictly confidential, and without the Company's written permission, you may not directly or indirectly disclose, use, copy, reproduce, adapt, modify, distribute, or disseminate the Release, in whole or in part, in any manner or form, or for any purpose.

By attending this Release and/or receiving, obtaining, or recording any materials, you agree to comply with the above confidentiality and non-disclosure obligations. Upon the Company's request, you shall return all copies of any materials to the Company.

You acknowledge that any breach or violation of the confidentiality obligations mentioned in this notice may cause irreparable harm and loss to the Company, including but not limited to reputational damage, damage to the Chow Tai Fook brand, and/or financial loss.

The Company reserves the right to pursue legal action for any breach or violation of the confidentiality obligations and the resulting damages.