Policy on Combating Financial Crimes

Our Commitment

The Bank's Policy on Combating Financial Crimes (PCFC) reflects our unwavering commitment to safeguarding the integrity of the financial system. We have established a comprehensive framework to prevent, detect, and respond to financial crimes such as money laundering, terrorist financing, sanctions breaches, bribery, and the financing of weapons of mass destruction.

Foundational Principles and Governance

We adhere to a **zero-tolerance approach** toward financial crimes. Our governance structure follows a three-lines-of-defence model:

- **First line:** Business and operations teams implement controls.
- **Second line:** AML Monitoring and Compliance provide oversight and policy guidance.
- **Third line:** Internal Audit independently assesses the effectiveness of these controls.

Oversight is reinforced through committees such as the Audit Committee of the Board (ACB), the Operational Risk Management Committee (ORMC), and the KYC Review Committee. These bodies ensure that the policy is implemented, periodically reviewed, and updated in line with evolving regulatory expectations.

Scope and Applicability

This policy applies to all domestic and international operations of the Bank, including International Business Units (IBUs) and offshore offices. While IBUs in GIFT City follow IFSCA-specific AML/KYC guidelines, subsidiaries operate under applicable local regulations, all within a group-wide risk management framework approved by the Board.

Objectives

- Prevent misuse of the Bank's products, services, and channels for financial crimes.
- Establish robust AML/CFT procedures across all operations.
- Ensure full compliance with applicable laws and regulatory directives.
- Support law enforcement agencies in investigating and prosecuting financial crimes.
- Train employees in recognizing and responding to financial crime risks.

Key Procedures

Customer Due Diligence and Risk Management

We follow a risk-based approach to customer onboarding and transaction monitoring. Customers are accepted only after thorough due diligence, including identity verification using officially valid documents, Aadhaar-based authentication, and video-based KYC (V-CIP). High-risk customers and transactions are subject to enhanced scrutiny.

We prohibit relationships with anonymous or fictitious entities, sanctioned individuals or organizations, and shell banks. All customers are screened against multiple sanctions lists, including those issued by the RBI, UN Security Council, OFAC, and internal watchlists. Any matches are escalated to the Financial Intelligence Unit (FIU-IND).

The Four Pillars of Financial Crime Prevention

1. **Customer Acceptance:**
   Only legitimate and verifiable customers are onboarded after a thorough evaluation of background, purpose, and expected transaction behavior. Special attention is given to politically exposed persons (PEPs), who require explicit approval from senior-level authorities and ongoing monitoring.

2. **Customer Identification:**
   We use multiple methods to verify identity, including Aadhaar-based eKYC, offline Aadhaar verification, officially valid documents (OVDs), video-based Customer Identification Process (V-CIP), Central KYC Registry (CKYC), and third-party due diligence. Identity verification is completed before any financial transaction is permitted.

3. **Risk Management:**
   Each customer is profiled based on risk perception, considering geography, occupation, transaction patterns, and product usage. Customers are categorized into low, medium, or high-risk segments. High-risk customers undergo enhanced due diligence, including deeper background checks and periodic reviews. A dynamic risk alert system generates triggers based on unusual activity.

4. **Monitoring of Transactions:**
   The AML Monitoring Department oversees surveillance of customer transactions, including Cash Transaction Reports (CTR), Suspicious Transaction Reports (STR), Counterfeit Currency Reports (CCR), Non-Profit Organization Reports (NPOR/NTR), and Cross-Border Wire Transfer Reports (CWTR). All suspicious activities are reported to FIU-IND in accordance with regulatory timelines. Automated systems screen transactions against sanctions lists and behavioral anomalies, with enhanced monitoring for high-risk categories.

Terrorist and Unlawful Activities Prevention

We do not open accounts for individuals or entities appearing on United Nations Security Council (UNSC) terrorist lists. We strictly follow the procedure for freezing assets under Section 51A of the Unlawful Activities Prevention Act (UAPA), 1967, as per government orders.

Sanctions Compliance

We comply with sanctions issued by the United Nations Security Council, OFAC, the Reserve Bank of India (RBI), and other relevant authorities. All customers and transactions are screened against multiple sanctions and watch lists at onboarding, during periodic reviews, and in real-time for transactions. Any match with a sanctioned entity triggers immediate escalation and reporting to FIU-IND.

Anti-Bribery and Corruption (ABC)

Bribery is defined as offering, giving, receiving, or soliciting anything of value to influence the actions of an official or person in a position of trust. In India, the Prevention of Corruption Act, 1988 (POCA) serves as the primary legislation governing bribery and corruption.

Our Anti-Bribery and Corruption framework is designed to prevent, detect, and respond to corrupt practices. We prohibit bribery, facilitation payments, and political donations undertaken by or on behalf of the Bank. Employees are trained to identify red flags and report suspicious behavior. We ensure that our partners and vendors adhere to anti-corruption standards, and we maintain whistleblower mechanisms.

The Bank also aligns its practices with international standards, including The OECD Convention on Combating Bribery of Foreign Public Officials, The ICC Rules on Combating Corruption (2011), The United Nations Convention Against Corruption (UNCAC).

Weapons of Mass Destruction (WMD) Financing

We are committed to preventing involvement in activities that support the proliferation of nuclear, biological, or chemical weapons. We comply with international treaties and Indian law, including the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005. Enhanced due diligence, transaction monitoring, and reporting are mandated for entities suspected of involvement in WMD proliferation.

Preservation of Records

We maintain records (hard and soft copies) of all transactions and customer identity information for at least five years from the date of cessation of the relationship, as required by law. This ensures that we can reconstruct individual transactions and support regulatory investigations.

Transparency and Public Disclosure

We publish our KYC standards and the list of acceptable documents on our corporate website. Customers are informed about the purpose of KYC and their rights under applicable laws.

Review and Continuous Improvement

The PCFC is reviewed annually by the Compliance Department and approved by the Board. Interim guidelines may be issued to address regulatory changes, ensuring that the policy remains current and effective.