FinTech AI Advisor Corp - Company Policies & Procedures

Document Version: 3.5
Effective Date: 2025-01-15
Last Reviewed: 2025-04-13

Table of Contents:

1. Introduction

This document outlines key operational policies for FinTech AI Advisor Corp ("the Company"). All employees, contractors, and automated systems, including the AI Advisor Bot ("the Bot"), must adhere to these guidelines. The purpose is to ensure regulatory compliance (including Sri Lanka regulations where applicable), ethical conduct, client protection, data security, and operational resilience.

2. Investment Suitability & Risk Assessment Policy

2.1. **Client Profiling:** A comprehensive client profile must be established before providing any personalized advice. This includes, but is not limited to:
 * Financial Situation (income, expenses, assets, liabilities)
 * Investment Objectives (e.g., capital preservation, income generation, growth, speculation)
 * Time Horizon (short, medium, long-term)
 * Risk Tolerance (qualitative assessment and quantitative scoring via CRPQ v2.5)
 * Liquidity Needs (access to funds required)
 * Investment Knowledge & Experience
 * Age and Dependents
 * ESG Preferences (Environmental, Social, Governance criteria)
2.2. **Risk Tolerance Levels:** Clients are categorized (Conservative, Moderate, Balanced Growth, Growth, Aggressive Growth). The methodology is documented in CRPQ v2.5 Scoring Guide.
2.3. **Product Risk Rating:** All investment products offered must have an internal risk rating assigned (Low, Medium-Low, Medium, Medium-High, High).
2.4. **Suitability Matching:** Recommendations must align client risk level with product risk rating. High-risk products are generally unsuitable for Conservative clients. Complex products (derivatives, structured notes) require enhanced suitability checks and client attestations of understanding.
2.5. **AI Suitability Engine:** The Bot uses a rules-based engine (SuitabilityCheck v3.0) integrated with the client profile database to perform initial suitability checks. Flags require human review.
2.6. **Regular Review:** Client profiles and suitability should be reviewed at least annually or upon significant changes in client circumstances or market conditions.
2.7. **Documentation:** Rationale for recommendations, especially those deviating slightly or involving complex products, must be meticulously documented in the CRM.

3. Data Privacy & Security Policy

3.1. **Compliance:** Adherence to GDPR, CCPA, Sri Lanka Personal Data Protection Act (PDPA) No. 9 of 2022, and other applicable data protection laws is mandatory.

3.2. **Data Inventory:** Maintain an inventory of Personal Identifiable Information (PII) collected, processed, and stored, including data types, purpose, location, and access controls.
3.3. **Lawful Basis:** Ensure a valid lawful basis (e.g., consent, contract necessity, legal obligation) exists for all PII processing activities.
3.4. **Client Rights:** Procedures must be in place to handle client requests regarding access, rectification, erasure ('right to be forgotten'), portability, and objection to processing their PII, respecting PDPA timelines.
3.5. **Consent Management:** Utilize a robust system for obtaining, recording, and managing client consent. Withdrawal of consent must be easy and promptly actioned.
3.6. **Data Minimization & Purpose Limitation:** Collect only necessary data for specified, explicit, and legitimate purposes. Do not process data beyond its original intended purpose without justification and/or additional consent.
3.7. **Access Control:** Role-based access controls (RBAC) enforced. Regular access reviews conducted quarterly. Multi-factor authentication (MFA) required for accessing sensitive systems.
3.8. **Encryption:** TLS 1.2+ for data in transit. AES-256 or stronger encryption for PII at rest. Key management policies must be strictly followed.
3.9. **Third-Party Risk:** Due diligence performed on all third-party vendors accessing or processing client data. Data Processing Agreements (DPAs) must be in place.
3.10. **Data Retention & Disposal:** Follow Data Retention Schedule (DRS-2025). Secure data disposal methods (e.g., cryptographic erasure, physical destruction) must be used.
3.11. **Privacy by Design:** Privacy considerations integrated into the design and development of new systems, products, and features, including AI models.

4. Communication Policy

4.1. **Accuracy & Timeliness:** Information provided must be factually correct and up-to-date based on available reliable sources (see `latest_updates.csv` usage protocol). Market commentary must be clearly dated.
4.2. **AI Disclosure:** Clear and persistent disclosure that the user is interacting with an AI, with an easy option to request human intervention.
4.3. **Language:** Use clear, simple language. Avoid overly technical terms. If technical terms are necessary, provide explanations.
4.4. **Marketing Communications:** Must comply with advertising standards and regulations. Performance data must be presented fairly, including relevant disclosures and risk warnings. Opt-out mechanisms must be honored.
4.5. **Record Keeping:** Chat logs, email communications, and summaries of substantive calls are automatically archived in the CRM and linked to the client profile. Retention as per DRS-2025.
4.6. **Prohibited Guarantees:** Explicitly forbidden to guarantee returns, specific price targets, or account values. Use appropriate disclaimers

regarding market risk and volatility.

5. Code of Ethics & Conduct

5.1. **Primacy of Client Interests:** Client interests must always take precedence over the interests of the Company or the employee/advisor.
5.2. **Due Care:** Exercise diligence, skill, and care in all professional activities.
5.3. **Confidentiality:** Client information is strictly confidential and may only be shared internally on a need-to-know basis or externally as required by law/regulation or with explicit client consent.
5.4. **Professionalism:** Maintain a high standard of professional conduct. Avoid any behavior that could discredit the Company or the financial services industry.
5.5. **Disclosure of Conflicts:** Disclose all material conflicts of interest (e.g., incentives for selling specific products, personal holdings in recommended securities) promptly and clearly. Maintain a Conflicts of Interest Register.
5.6. **Gifts & Entertainment:** Adhere to the Gifts & Entertainment Policy (GEP-2024) limits to avoid perceived or actual conflicts.

6. Fee Disclosure Policy

6.1. **Clarity:** Fee structures must be simple and easy to understand. All potential charges (advisory fees, platform fees, transaction costs, fund expense ratios, third-party fees) must be disclosed.
6.2. **Timing:** Full fee disclosure (FS-2025-Q2) provided *before* a client signs an agreement or makes an investment.
6.3. **Changes:** Clients must be notified at least 30 days in advance of any changes to the standard fee schedule.
6.4. **Billing:** Invoices or account statements must clearly itemize all fees charged during the period.

7. Complaint Handling Procedure

7.1. **Channels:** Clients can submit complaints via email (complaints@fintechadvisor.lk), secure message via app/portal, or registered post.
7.2. **Logging:** All complaints logged centrally by the Compliance Department, assigned a unique tracking number.
7.3. **Acknowledgement:** Written acknowledgement sent within 2 business days, outlining the process and expected timeline.

7.4. **Investigation:** Impartial investigation conducted by Compliance, potentially involving relevant departments/individuals. Records gathered.
7.5. **Resolution:** Formal written response within 15 business days detailing findings and any redress/action offered. If complex, provide an update and revised timeline.
7.6. **Escalation:** Inform clients of their right to escalate the complaint to relevant external bodies (e.g., Financial Ombudsman) if unsatisfied with the resolution.
7.7. **Root Cause Analysis:** Complaints analyzed periodically to identify systemic issues or trends requiring corrective action.

8. Anti-Money Laundering (AML) & Counter-Terrorist Financing (CTF) Policy

8.1. **MLRO:** Designated Money Laundering Reporting Officer (MLRO) with defined responsibilities.
8.2. **Risk-Based Approach:** Apply a risk-based approach to CDD. Enhanced Due Diligence (EDD) required for high-risk clients (e.g., PEPs, clients from high-risk jurisdictions).
8.3. **KYC/CDD:** Verify client identity using reliable, independent source documents/data. Understand the nature and purpose of the business relationship. Identify beneficial owners where applicable. Ongoing monitoring of client activity.
8.4. **Sanctions Screening:** Screen clients against relevant international and local sanctions lists at onboarding and periodically.
8.5. **Suspicious Activity Monitoring:** Monitor transactions for unusual patterns or activities inconsistent with the client's profile. Examples: large cash deposits, rapid movement of funds, unexplained complex structures, transactions involving high-risk jurisdictions.
8.6. **SAR Filing:** File Suspicious Activity Reports with the Financial Intelligence Unit (FIU) of Sri Lanka promptly when suspicion arises. Maintain confidentiality regarding SAR filings ('tipping off' is prohibited).
8.7. **Training:** Mandatory annual AML/CTF training for all relevant staff. Records maintained.

9. Cybersecurity Awareness & Incident Response

9.1. **Employee Responsibility:** Employees are the first line of defense. Must complete mandatory security awareness training annually. Must report suspicious emails, calls, or system behavior immediately to IT Security.
9.2. **Password Policy:** Strong, unique passwords required. MFA enforced where possible. Passwords must not be shared.
9.3. **Phishing & Malware:** Be vigilant against phishing attempts. Do not click suspicious links or open unexpected attachments. Use company-approved antivirus software.

9.4. **Acceptable Use:** Company IT resources are for business purposes. Use of unauthorized software or devices is prohibited. Adhere to the Acceptable Use Policy (AUP-2024).
9.5. **Incident Response Plan (IRP):** Follow the IRP (IRP-2025-v2) in case of a suspected or confirmed security incident (e.g., data breach, malware infection, denial-of-service). Key steps: Containment, Eradication, Recovery, Post-Incident Analysis. Designated incident response team activated via IT Security Helpdesk.

10. Business Continuity & Disaster Recovery (BCDR) Plan Summary

10.1. **Objective:** Ensure critical business functions, including client support and trading capabilities, can resume within defined Recovery Time Objectives (RTOs) following a disruptive event (e.g., natural disaster, power outage, cyberattack).
10.2. **Risk Assessment:** Business Impact Analysis (BIA) and risk assessments conducted regularly to identify critical systems and potential threats.
10.3. **Recovery Strategies:** Includes data backups (off-site, immutable), redundant infrastructure (cloud-based failover), alternate work locations/remote work capabilities, and emergency communication procedures.
10.4. **Testing:** BCDR plan tested at least annually through simulations or tabletop exercises. Results documented, and plan updated.
10.5. **AI Bot Resilience:** The Bot's infrastructure designed for high availability with redundancy across multiple zones/regions. Critical data required for operation is backed up frequently.

11. Record Keeping Policy

11.1. **Regulatory Requirements:** Maintain records as required by financial regulations (e.g., client agreements, transaction records, communications, suitability assessments, AML documentation) for the minimum prescribed periods (often 6-7 years or longer). Refer to DRS-2025.
11.2. **Format & Storage:** Records maintained in a secure, durable, and easily retrievable format (primarily digital). Ensure integrity and authenticity. Use WORM (Write Once, Read Many) storage where appropriate for regulatory data.
11.3. **Accessibility:** Records must be accessible to authorized personnel and regulators upon request within reasonable timeframes.
11.4. **Disposal:** Secure disposal of records after the retention period expires, following methods outlined in the Data Privacy policy.

12. Social Media Policy for Employees

12.1. **Scope:** Applies to professional and personal use of social media where it relates to or could impact the Company.
12.2. **Confidentiality:** Do not disclose confidential client or company information on social media.
12.3. **Professionalism:** Maintain professionalism online. Avoid making inappropriate comments or engaging in activities that could damage the Company's reputation.
12.4. **Endorsements/Recommendations:** Do not provide specific investment advice or recommendations via personal social media accounts. Official company channels are managed by the Marketing department.
12.5. **Disclaimers:** If identifying as an employee, consider using a disclaimer stating views are personal and not those of the Company.

13. Cross-Border Business Policy

13.1. **Authorization:** Only conduct business with clients in jurisdictions where the Company is appropriately licensed and registered. Maintain a list of authorized jurisdictions.
13.2. **Compliance:** Adhere to the specific regulatory requirements of each jurisdiction where business is conducted, including rules on marketing, product suitability, and taxation.
13.3. **AI Limitations:** The Bot must be configured to recognize client jurisdiction (based on verified profile data) and avoid providing advice or promoting products not permitted in that jurisdiction.

14. Policy Review & Updates

14.1. **Schedule:** All policies reviewed at least annually by the relevant department head and the Compliance department.
14.2. **Triggers for Review:** Reviews may also be triggered by regulatory changes, significant business changes, audit findings, or major incidents.
14.3. **Approval:** Material changes require approval from the Senior Management Committee and/or Board of Directors.
14.4. **Communication:** Updated policies communicated to all relevant staff. Training provided on significant changes. Policies accessible via the company intranet.
