GLOBAL PRIME FX

CORPORATE COMPLIANCE HANDBOOK

Internal Operations & Compliance Manual

Document Classification	CONFIDENTIAL – Internal Use Only
Version	1.0
Effective Date	12 May 2018
Status	Internal – Controlled Document
Document Owner	Chief Compliance Officer
Review Cycle	Annual or upon material regulatory change

This document is an internal operations and compliance manual intended solely for the use of Global PrimeFX employees, officers, and authorised agents. It is not an official public policy statement, regulatory filing, or customer-facing document.

1. DOCUMENT CONTROL

This Corporate Compliance Handbook is a controlled document. Unauthorised copies, distribution, or modification are prohibited. All printed copies are considered uncontrolled unless stamped and logged by the Compliance Department.

1.1 Document Information

Field	Detail
Document Title	Global PrimeFX Corporate Compliance Handbook
Document Reference	GPFX-COMP-HB-001
Version	1.0
Issue Date	12 May 2018
Next Scheduled Review	May 2019
Classification	CONFIDENTIAL – Internal Use Only
Distribution	All staff (via secure internal portal); Compliance & Senior Management hard copies

1.2 Amendment Procedure

Any proposed amendment to this Handbook must be submitted in writing to the Chief Compliance Officer (CCO). Material changes require approval by the Compliance Committee and, where applicable, the Board Risk & Compliance Committee. Minor administrative updates may be authorised by the CCO. All changes are recorded in the Revision History section.

2. CONFIDENTIALITY NOTICE

This Handbook and all related materials are the exclusive property of Global PrimeFX and contain confidential and proprietary information. Access is restricted to authorised personnel only.

Recipients must:

- Store the document securely (electronic copies on approved systems only; physical copies in locked cabinets).
- Not copy, distribute, or disclose any part of this Handbook to external parties without prior written authorisation from the CCO.
- Report any suspected unauthorised access or loss of the document immediately to Compliance.
- Return or securely destroy all copies upon termination of employment or cessation of authorised access.
- Treat all customer data, internal controls descriptions, and risk methodologies as strictly confidential.

Breach of confidentiality may result in disciplinary action up to and including termination of employment and, where applicable, civil or criminal liability.

3. TABLE OF CONTENTS

4. EXECUTIVE SUMMARY

Global PrimeFX is committed to the highest standards of regulatory compliance, ethical conduct, and operational integrity. This Corporate Compliance Handbook consolidates the firm's core policies, procedures, and control frameworks that govern day-to-day operations and risk management.

The Handbook is designed to:

- Provide a single, authoritative reference for all staff on compliance expectations and mandatory procedures.
- Support a culture of integrity, transparency, and accountability across the organisation.
- Ensure consistent application of Customer Due Diligence (CDD/KYC), Anti-Money Laundering (AML), and counter-terrorist financing measures in line with applicable laws and industry best practice.
- Define clear escalation paths, roles, and responsibilities for compliance-related matters.
- Protect the firm, its clients, and its reputation by embedding robust operational and information-security controls.

All employees, contractors, and authorised agents are required to read, understand, and adhere to the requirements set out in this Handbook. Non-compliance may result in disciplinary action and, where relevant, regulatory or legal consequences.

This is an internal operations manual. It does not constitute legal advice, a public policy statement, or a substitute for specific regulatory guidance applicable in any jurisdiction in which Global PrimeFX operates or is licensed.

5. PURPOSE & SCOPE

5.1 Purpose

The purpose of this Handbook is to establish a coherent, practical, and enforceable framework of compliance policies and operational procedures that enable Global PrimeFX to meet its legal, regulatory, and ethical obligations while delivering high-quality services to clients.

5.2 Scope

This Handbook applies to:

- All permanent and temporary employees of Global PrimeFX and its controlled affiliates.
- Directors, officers, and members of the Board and Board committees.
- Contractors, consultants, and third-party service providers who have access to firm systems or client data, to the extent their contractual obligations require adherence to firm policies.
- All business activities, products, and services offered by Global PrimeFX, including but not limited to spot FX, CFDs, and related trading and payment services.

5.3 Regulatory Context

Global PrimeFX operates under applicable financial services regulations in the jurisdictions in which it is authorised. Staff must remain aware that regulatory requirements may differ by product, client type, and geography. Where local law imposes stricter requirements than those set out in this Handbook, the stricter standard prevails. The Compliance Department maintains a regulatory inventory and issues jurisdiction-specific guidance as needed.

6. CORPORATE GOVERNANCE

Sound corporate governance underpins the firm's ability to manage risk, meet regulatory expectations, and protect stakeholder interests. Global PrimeFX maintains a clear organisational structure with defined lines of accountability and independent oversight functions.

6.1 Board Oversight

The Board of Directors holds ultimate responsibility for the firm's strategy, risk appetite, and compliance culture. The Board Risk & Compliance Committee (or equivalent) receives regular reports from the Chief Compliance Officer and Internal Audit on the effectiveness of the compliance framework, material incidents, and emerging regulatory risks.

6.2 Three Lines of Defence

Global PrimeFX operates a Three Lines of Defence model:

- **First Line** – Business units and operational teams own and manage risks arising from their activities and are responsible for implementing day-to-day controls.
- **Second Line** – Compliance, Risk Management, and related control functions provide independent oversight, policy setting, monitoring, and advisory support.
- **Third Line** – Internal Audit provides independent assurance to the Board and senior management on the effectiveness of governance, risk management, and internal controls.

6.3 Compliance Culture

Senior management is expected to set the tone from the top. All managers must promote ethical behaviour, encourage the raising of concerns, and ensure that compliance considerations are integrated into business decisions. Retaliation against individuals who raise genuine compliance concerns in good faith is strictly prohibited.

7. ROLES & RESPONSIBILITIES

Clear allocation of responsibilities is essential for effective compliance. The following roles carry specific obligations under this Handbook.

Board of Directors / Board Risk & Compliance Committee

Approve the overall compliance framework and risk appetite; receive and act upon material compliance reports; ensure adequate resources for the compliance function.

Chief Executive Officer (CEO)

Foster a culture of compliance; ensure the firm's strategy is consistent with regulatory obligations and ethical standards; support the independence of the Compliance function.

Chief Compliance Officer (CCO)

Own and maintain this Handbook; design and oversee the compliance programme; advise the business; monitor adherence; report to the Board; act as primary regulatory contact where designated.

Money Laundering Reporting Officer (MLRO) / AML Compliance Officer

Oversee the AML/CFT framework; receive and assess internal suspicious activity reports; make external disclosures where required; maintain AML policies and training.

Heads of Business / Department Managers

Implement policies within their areas; ensure staff complete required training; escalate issues promptly; embed compliance into operational processes.

All Employees and Authorised Agents

Read and comply with this Handbook and related procedures; complete mandatory training; report concerns and potential breaches without delay; protect client and firm confidential information.

Internal Audit

Provide independent assurance on the design and operating effectiveness of compliance and operational controls; report findings to the Board Audit Committee.

8. CODE OF CONDUCT

All personnel are expected to act with integrity, professionalism, and in the best interests of clients and the firm. The following principles form the foundation of expected behaviour.

8.1 Core Principles

Integrity: Act honestly and ethically in all dealings. Do not engage in or facilitate any form of fraud, market abuse, bribery, or corruption.

Client Focus: Treat clients fairly. Provide clear, accurate, and not misleading information. Avoid conflicts of interest or manage them transparently.

Compliance with Laws: Comply with all applicable laws, regulations, and internal policies. When in doubt, seek guidance from Compliance before acting.

Confidentiality: Protect client and firm information. Do not use confidential information for personal gain or disclose it without proper authority.

Professionalism: Maintain high standards of competence and conduct. Respect colleagues and avoid behaviour that could harm the firm's reputation.

Speaking Up: Raise concerns about potential misconduct, breaches, or unethical behaviour through established channels without fear of retaliation.

8.2 Conflicts of Interest

Personnel must identify, disclose, and manage actual or potential conflicts of interest. Personal trading, outside business interests, and gifts & hospitality are subject to specific policies and pre-approval requirements where applicable. Undisclosed conflicts may constitute serious misconduct.

8.3 Market Conduct

Global PrimeFX prohibits market abuse, including insider dealing, unlawful disclosure of inside information, and market manipulation. Staff involved in trading or client order handling must adhere to best-execution and order-handling standards and report any suspicion of abusive activity.

9. CUSTOMER DUE DILIGENCE (KYC)

Robust Customer Due Diligence is a cornerstone of the firm's AML/CFT and fraud-prevention framework. No account may be opened or significant transaction processed without completion of the required CDD measures appropriate to the risk profile of the client.

9.1 Core CDD Requirements

- Identify the client and verify identity using reliable, independent source documents, data, or information.
- Identify beneficial owners and take reasonable measures to verify their identity.
- Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
- Conduct ongoing monitoring of the business relationship, including scrutiny of transactions to ensure consistency with the client's profile and risk assessment.
- Apply enhanced due diligence (EDD) for higher-risk clients, including PEPs, clients from high-risk jurisdictions, and complex ownership structures.

9.2 Risk-Based Approach

CDD intensity is calibrated to the assessed money-laundering and terrorist-financing risk of the client and product. Risk factors include geography, client type, delivery channel, product features, and transaction patterns. The firm maintains a documented risk-assessment methodology that is reviewed periodically.

9.3 Onboarding Controls

Account opening is subject to a defined workflow that includes automated and manual checks, sanctions and PEP screening, and, where required, secondary review by Compliance or a designated approver. Accounts may not be activated until CDD is complete and any outstanding queries are resolved.

9.4 Ongoing Monitoring & Periodic Review

Client files are subject to periodic review according to risk rating (e.g., higher-risk clients more frequently). Trigger events such as material changes in activity, adverse media, or regulatory alerts also initiate reviews. Incomplete or outdated CDD may result in account restrictions or exit.

10. ANTI-MONEY LAUNDERING (AML) CONTROLS

Global PrimeFX maintains a comprehensive AML and Counter-Terrorist Financing (CTF) programme designed to detect, prevent, and report suspected money laundering and terrorist financing activity.

10.1 Key Components

Risk Assessment: Enterprise-wide and client-level ML/TF risk assessments inform control design and resource allocation.

Policies & Procedures: Documented AML policies covering CDD, transaction monitoring, sanctions screening, suspicious activity reporting, and record keeping.

Sanctions & Watchlist Screening: Real-time and batch screening of clients and relevant counterparties against applicable sanctions lists and internal watchlists.

Transaction Monitoring: Automated and manual monitoring systems to identify unusual or potentially suspicious patterns.

Suspicious Activity Reporting: Clear internal escalation to the MLRO and external reporting to the competent authorities in accordance with local requirements.

Training: Role-appropriate AML training for all relevant staff, with enhanced training for higher-risk roles.

Independent Testing: Periodic independent review of the AML programme by Internal Audit or external specialists.

10.2 Prohibited Activities

The firm does not knowingly facilitate money laundering, terrorist financing, or the evasion of sanctions. Staff must not process transactions where they know or suspect such activity, and must escalate immediately to the MLRO. Tipping-off a client about an internal investigation or external report is strictly prohibited.

10.3 MLRO Authority

The MLRO has the authority and independence to investigate and escalate matters, including the ability to recommend account restrictions or exit, without requiring business-unit approval. Material cases are reported to senior management and, where appropriate, the Board.

11. OPERATIONAL RISK MANAGEMENT

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events. Global PrimeFX maintains a structured approach to identifying, assessing, mitigating, monitoring, and reporting operational risk.

11.1 Risk Identification & Assessment

Business units are responsible for identifying operational risks inherent in their processes. Risk and Control Self-Assessments (RCSAs), process mapping, and incident analysis are used to evaluate inherent and residual risk levels. Key risk indicators (KRIs) are monitored and reported.

11.2 Control Environment

Controls include segregation of duties, dual authorisation for sensitive actions, system access controls, reconciliations, exception reporting, and documented procedures. Control effectiveness is tested periodically by the first and second lines and assured by Internal Audit.

11.3 Incident Management

Operational incidents (including near misses) must be logged promptly in the firm's incident management system. Root-cause analysis is performed for material events, and remedial actions are tracked to closure. Significant incidents are escalated to senior management and, where required, to regulators.

12. WITHDRAWAL REVIEW WORKFLOW

Client withdrawals are subject to a defined review and approval workflow designed to mitigate fraud, money-laundering, and operational risk while providing timely service to legitimate clients.

12.1 Standard Process

Step 1: Client submits a withdrawal request through an approved channel (client portal or authorised form).

Step 2: System performs automated checks: available balance, account status, outstanding holds, sanctions/PEP re-screening where configured, and basic pattern analysis.

Step 3: Operations / Payments team reviews the request against client profile, source of funds information, and any active alerts.

Step 4: Additional verification (e.g., identity re-confirmation, source-of-funds evidence) is requested where risk indicators are present.

Step 5: Approval is granted according to the firm's dual-control and authority matrix (based on amount and risk).

Step 6: An activated Transfer Code must be in place before funds can be released (see section 12.4).

Step 7: Payment is executed via approved banking channels; confirmation is provided to the client.

Step 8: Records of the request, checks performed, and approvals are retained in accordance with the Record Retention Policy.

12.2 Escalation Triggers

Requests that trigger predefined risk rules (e.g., large first-time withdrawal, mismatch with declared profile, adverse media, or unusual velocity) are escalated to Compliance or a designated senior approver before processing. Staff must not override system blocks without documented authorisation.

12.3 Client Communication

Clients are informed of expected processing times and any additional information required. Delays caused by compliance reviews are handled professionally and without disclosing the existence of any suspicious activity investigation (to avoid tipping-off).

12.4 Transfer Code Requirement

To enhance the security of withdrawal transactions, all approved withdrawals require an activated Transfer Code before funds can be released. The Transfer Code serves as an additional authentication and authorisation control. Funds will not be released until a valid, activated Transfer Code associated with the client account and the specific withdrawal request is confirmed by the Payments / Operations team (or automated system controls where configured).

Staff must verify the status of the Transfer Code as part of the pre-release checklist. Any attempt to process a withdrawal without a confirmed activated Transfer Code is a control breach and must be escalated immediately.

12.5 Withdrawal Fees

Withdrawal-related charges, including the purchase or activation of a Transfer Code where applicable, must be paid separately. These charges cannot be deducted from the available account balance during the withdrawal process.

Operations and Payments staff must ensure that any applicable fees are settled through the designated payment channel before or independently of the withdrawal release. Clients should be clearly informed of fee requirements at the time of the withdrawal request. Failure to collect required fees separately does not authorise deduction from the withdrawal amount.

12.6 Security Verification

Clients may also be required to complete identity verification (KYC) before withdrawals are processed. This may include refreshed or enhanced due diligence where the existing CDD file is incomplete, outdated, or where risk indicators warrant additional verification.

Where security verification is required, the withdrawal remains on hold until satisfactory evidence is received and reviewed. Staff must not release funds solely on the basis of a prior KYC status if a current verification request is outstanding. All verification steps and outcomes are documented in the client file and the withdrawal workflow record.

13. INFORMATION SECURITY & DATA PROTECTION

Protecting client and firm data is a core obligation. Global PrimeFX maintains technical, organisational, and procedural controls aligned with industry standards and applicable data-protection laws.

13.1 Key Principles

- Data is classified according to sensitivity and handled accordingly.
- Access is granted on a need-to-know and least-privilege basis and is regularly reviewed.
- Strong authentication, encryption in transit and at rest (where appropriate), and secure configuration baselines are applied.
- Staff must not share credentials, leave systems unlocked, or transfer sensitive data via unapproved channels.
- Personal data is processed lawfully, fairly, and transparently, and only for specified purposes.
- Data subject rights (access, rectification, erasure, etc.) are handled in accordance with applicable law and internal procedures.

13.2 Acceptable Use & Endpoint Security

Firm systems and devices are for authorised business use. Installation of unapproved software, use of personal cloud storage for firm data, and connection of unauthorised devices are prohibited. Suspected security incidents (malware, phishing, unauthorised access) must be reported immediately to IT Security and Compliance.

13.3 Third-Party & Cloud Risk

Vendors that process or store firm or client data are subject to due diligence, contractual data-protection clauses, and ongoing monitoring commensurate with the risk. Material outsourcing arrangements are approved through the firm’s governance process.

14. CUSTOMER COMMUNICATION STANDARDS

All client communications must be clear, fair, and not misleading. Staff must adhere to approved templates and channels where mandated, and escalate complex or sensitive matters appropriately.

14.1 Principles

- Use plain language appropriate to the client's level of understanding.
- Ensure promotional and educational materials are accurate, balanced, and compliant with applicable advertising rules.
- Record and retain client communications (including chat, email, and calls) in accordance with regulatory and internal requirements.
- Do not provide personalised investment advice unless specifically authorised and qualified to do so.
- Handle complaints promptly, fairly, and in line with the firm's complaints procedure; escalate systemic issues.
- Never disclose internal compliance investigations or SAR-related information to clients.

14.2 Social Media & External Statements

Only authorised spokespersons may make public statements on behalf of Global PrimeFX. Personal social-media activity must not disclose confidential information or create the impression of speaking for the firm without authorisation.

15. INCIDENT REPORTING & ESCALATION

Timely identification and escalation of incidents is critical to containing harm and meeting regulatory notification obligations.

15.1 What Must Be Reported

- Suspected or actual breaches of law, regulation, or internal policy.
- Suspected money laundering, fraud, market abuse, or sanctions violations.
- Operational incidents causing or potentially causing client detriment, financial loss, or reputational harm.
- Information-security incidents, including data breaches and successful phishing.
- Complaints indicating possible systemic issues or serious misconduct.
- Conflicts of interest that cannot be managed under existing arrangements.

15.2 How to Report

Incidents should be reported through the firm's designated channels (incident management system, Compliance mailbox, or MLRO escalation line). In urgent cases, staff should contact their manager and Compliance immediately by telephone, followed by formal logging. Whistleblowing channels are available for concerns that staff prefer to raise confidentially.

15.3 Escalation Matrix (Summary)

Severity / Type	Initial Escalation	Further Escalation
Routine operational issue	Line Manager / Ops Lead	Head of Operations if unresolved
Compliance / AML concern	Compliance / MLRO	CCO → Board Committee if material
Security / data incident	IT Security + Compliance	CISO / CCO → Executive & regulators as required
Significant client harm / regulatory breach	CCO / CEO	Board; external notification per legal requirements

16. INTERNAL AUDIT & COMPLIANCE MONITORING

Independent assurance and ongoing monitoring are essential to verify that controls operate as designed and that the compliance framework remains effective.

16.1 Compliance Monitoring Programme

The Compliance function maintains a risk-based monitoring plan covering key regulatory obligations, including sample testing of CDD files, transaction monitoring alerts, communications, and training completion. Findings are reported to senior management with agreed remediation timelines.

16.2 Internal Audit

Internal Audit conducts independent reviews of governance, risk management, and control processes according to an annual plan approved by the Board Audit Committee. Audit reports and management actions are tracked to closure. Material unresolved issues are escalated to the Board.

16.3 Regulatory Examinations & Information Requests

All regulatory examinations, information requests, and on-site visits are coordinated through the Compliance function (or designated regulatory liaison). Staff must provide accurate and complete information and must not alter or destroy records that may be relevant to an inquiry.

17. RECORD RETENTION POLICY

Accurate and complete records support regulatory compliance, client service, and the firm's ability to demonstrate control effectiveness. Records must be retained for the periods required by applicable law and internal policy, and must be retrievable in a timely manner.

17.1 Illustrative Retention Periods

Record Category	Minimum Retention	Notes
Client identification & CDD files	At least 5 years after end of relationship (or longer if required locally)	Includes beneficial ownership data
Transaction records	At least 5 years	From date of transaction
Suspicious activity reports & related investigation files	At least 5 years (or as required by local law)	Secure restricted access
Communications (trading-related)	As required by applicable record-keeping rules (often 5–7 years)	Voice, chat, email
Training records	At least 5 years	Evidence of completion
Policy versions & Board papers	Permanent or long-term archive	Controlled repository

Where local law requires a longer retention period, the longer period applies. Secure destruction methods must be used when retention periods expire, and destruction must be logged.

18. STAFF TRAINING REQUIREMENTS

Competence is a regulatory expectation and a business necessity. All staff must complete mandatory compliance training appropriate to their role.

18.1 Mandatory Training

- Induction compliance training for all new joiners (including AML, Code of Conduct, information security, and this Handbook).
- Annual AML/CFT refresher training for all relevant staff.
- Role-specific training (e.g., enhanced AML for onboarding and monitoring teams; market-conduct training for trading staff).
- Periodic updates when material regulatory or policy changes occur.

18.2 Tracking & Consequences

Training completion is tracked centrally. Failure to complete mandatory training by the required deadline may result in restricted system access, escalation to management, and disciplinary measures. Managers are accountable for ensuring their teams complete required training.

19. BUSINESS CONTINUITY

Global PrimeFX maintains Business Continuity and Disaster Recovery plans to ensure the firm can continue critical operations and protect client interests in the event of significant disruption.

19.1 Key Elements

- Identification of critical business functions and recovery time objectives.
- Documented recovery procedures, alternate work arrangements, and communication protocols.
- Regular testing of continuity and disaster-recovery arrangements, with results reported to management.
- Dependency mapping for key third-party providers and contingency arrangements where feasible.
- Clear crisis-management structure and escalation paths.

All staff must familiarise themselves with their role-specific continuity responsibilities and participate in scheduled tests as required.

20. POLICY EXCEPTIONS

Exceptions to the requirements of this Handbook may be granted only in limited circumstances and under strict controls.

20.1 Process

- A written exception request must be submitted to the CCO (or delegate), describing the nature of the exception, business justification, risk assessment, compensating controls, and proposed duration.
- The CCO evaluates the request and may approve, approve with conditions, or reject it. Material or prolonged exceptions may require additional senior or Board-level approval.
- Approved exceptions are logged, time-limited, and subject to periodic review.
- Expired exceptions must be re-justified or the standard requirement reinstated.

Operating outside policy without an approved exception constitutes a breach and will be treated accordingly.

21. REVISION HISTORY

Version	Date	Author / Owner	Summary of Changes
1.0	12 May 2018	Chief Compliance Officer	Initial issue of the Corporate Compliance Handbook as a consolidated internal operations manual.

Future revisions will be recorded in this section. Staff will be notified of material updates and required to acknowledge revised versions as directed by Compliance.

22. COMPLIANCE APPROVAL PAGE

This Corporate Compliance Handbook (Version 1.0) has been reviewed and approved for issuance as an internal controlled document of Global PrimeFX.

Role	Name	Signature	Date
Chief Compliance Officer	_____	_____	_____
Chief Executive Officer	_____	_____	_____
Chair, Board Risk & Compliance Committee (or equivalent)	_____	_____	_____

23. SIGNATURE BLOCKS – STAFF ACKNOWLEDGEMENT

I acknowledge that I have received, read, and understood the Global PrimeFX Corporate Compliance Handbook (Version 1.0). I understand that I am required to comply with its requirements and that failure to do so may result in disciplinary action. I am aware of the channels available to raise questions or concerns.

Acknowledgement 1

Full Name: _____

Employee / Contractor ID: _____

Department / Role: _____

Signature: _____

Date: _____

Acknowledgement 2

Full Name: _____

Employee / Contractor ID: _____

Department / Role: _____

Signature: _____

Date: _____

Acknowledgement 3

Full Name: _____

Employee / Contractor ID: _____

Department / Role: _____

Signature: _____

Date: _____

— End of Global PrimeFX Corporate Compliance Handbook (Version 1.0) —

This document is confidential and intended for internal use only. It is not an official public policy or regulatory filing.