REGULATORY AND GOVERNANCE POLICIES

CONTENTS

COMPLIANCE WITH ACCOUNTING METHODS & DISCLOSURE POLICY

1. Purpose
This policy ensures the firm's financial records, reporting practices, and disclosures fully comply with applicable accounting standards, regulatory requirements, and internal transparency expectations. It also outlines how accounting systems are integrated with trading modules and the approach for disclosure of accounting methods.

2. Scope
This policy applies to all:

- Financial records and reporting functions
- Trading and back-office operations
- Relevant software systems and modules (accounting, trading, settlement)
- Employees involved in accounting, compliance, operations, and reporting

3. Regulatory Framework
The firm complies with:

- **International Financial Reporting Standards (IFRS)** as adopted in Pakistan
- **Companies Act, 2017**
- **Income Tax Ordinance, 2001**
- **SECP directives and PSX Rule Book**
- **Institute of Chartered Accountants of Pakistan (ICAP) Technical Releases**

PART I: ACCOUNTING METHOD DISCLOSURE
4. Accounting Methods Used

- The firm uses the **accrual basis** of accounting, where revenues and expenses are recognized when earned or incurred, regardless of when cash is received or paid.
- Assets are recorded at **historical cost**, unless stated otherwise.
- Fair value adjustments are made in accordance with applicable IFRS where required (e.g., for investments).
- Depreciation methods and useful lives are disclosed in the firm's annual audited financial statements.

5. Disclosure Practices

- All accounting policies, estimates, and judgments are disclosed in the **Notes to the Financial Statements**, which are reviewed and approved by the external auditor annually.
- Any **changes in accounting policy** or restatements are highlighted transparently in compliance with IAS 8.
- Disclosure is made for all related-party transactions, client asset segregation, revenue recognition, and commission arrangements.

PART II: SYSTEM INTEGRATION – TRADING & ACCOUNTING

6. System Integration Overview

Module	Integration Status	Platform
Trading System	Integrated	Connected to settlement and client ledgers
Accounting System	Partially Integrated	Manual input for non-trade income and expenses
Settlement Module	Integrated	Real-time posting of trades
Client Ledger System	Fully Integrated	Auto-update from trading module
HR/Payroll System	Standalone	Updated monthly via journal entries

7. Key Controls

- **Auto-Posting:** Executed trades automatically update client ledgers and brokerage revenue accounts.
- **Audit Trails:** Every transaction has a system-generated timestamp and user record.
- **Manual Reconciliations:** Conducted daily for modules that are not fully integrated (e.g., expenses, payroll).

- **Error Logs:** All failed transactions or mismatches are reviewed by the Operations/Finance department daily.

8. Oversight & Compliance

Function	Responsibility
Finance Department	Ensure accounting policies are followed and disclosed accurately
Compliance Officer	Review disclosure compliance and liaise with auditors/SECP
IT Department	Maintain secure, integrated system infrastructure
External Auditor	Validate appropriateness of accounting methods and disclosures annually

9. Training & Awareness

- Annual training is conducted for Finance and Operations teams on updates to accounting standards and system usage.
- New staff are trained on module interfaces and data entry protocols to ensure accuracy and consistency.

10. Policy Review

This policy shall be reviewed in 3 years or sooner if:

- New accounting standards are introduced
- System upgrades or integrations occur
- Required by SECP, PSX, or statutory auditors

BACKUP POLICY

1. Purpose
This policy outlines the procedures and frequency for backing up critical systems and data to ensure business continuity and data recovery in case of system failure, data loss, or disaster.

2. Scope
This policy applies to all critical data and systems of the firm, including but not limited to:

- Trading platform data
- Client records and transaction history
- Financial and operational data
- Regulatory and compliance documents
- Email systems and communications
- Backup of databases and file servers

3. Backup Frequency

Data Type	Backup Frequency	Retention Period
Trading Platform Data	**Daily** (End of Day backup)	6 months
Client and Transaction Records	**Daily** (Continuous or End of Day backup)	5 years
Financial and Operational Data	**Weekly** (Incremental backups)	5 years
Email System	**Daily** (Full backup)	3 months
Database Systems	**Hourly** (Incremental)	1 year
Critical Application Data	**Daily** (Full backup)	1 year
Backup for Disaster Recovery (Offsite)	**Weekly** (Full backup)	6 months

- **Real-Time Data Backup**: Critical systems (e.g., trading platform, database systems) require **real-time replication** for continuous protection, especially in live trading environments.

4. Backup Types

- **Full Backup**: A complete copy of all data and systems, taken at the scheduled time.
- **Incremental Backup**: A copy of only the data changed since the last backup, performed daily or hourly.
- **Offsite Backup**: Data is backed up and stored at a remote location (cloud or external storage) to ensure redundancy and disaster recovery capability.

5. Backup Storage

- All backup data shall be securely stored both **on-site** (in the firm's data center) and **off-site** (cloud or external storage).
- **Encryption** shall be used for both on-site and off-site storage to ensure data confidentiality.
- Backup media (e.g., tapes, hard drives) shall be stored in secure, fireproof, and environmentally controlled areas.

6. Backup Testing and Verification

- Backup systems must be regularly tested **quarterly** to ensure recoverability, functionality, and integrity.
- A **disaster recovery drill** shall be conducted atleast **annually** to simulate data restoration from backups.
- The IT Department will generate a **monthly backup report**, confirming successful backups and verifying that critical data has been backed up properly.

7. Roles and Responsibilities

Role	Responsibility
Head of IT	Ensure that backup procedures are followed and that backups are properly executed.
IT Department	Perform backups, monitor backup systems, and verify that backup schedules are followed.
Compliance Officer	Ensure backup practices comply with regulatory requirements and internal data protection policies.

Role	Responsibility
Disaster Recovery Team	Coordinate restoration processes in the event of data loss or system failure.

8. Data Retention and Destruction

- Data backups will be retained as per the **retention periods** specified in the backup frequency table.
- Once the retention period expires, backups will be securely destroyed using **data wiping** methods to prevent unauthorized access to sensitive information.

9. Policy Review

- This policy will be reviewed if there are significant changes in the IT environment, business operations, or regulatory requirements.

DISASTER RECOVERY AND BUSINESS CONTINUITY POLICY

1. Purpose
This policy establishes the procedures and guidelines for **Disaster Recovery (DR)** and **Business Continuity Planning (BCP)** to ensure that the firm can maintain critical operations, protect data, and recover quickly in the event of unforeseen disruptions, such as system failures, natural disasters, or cyber-attacks.

2. Scope
This policy applies to:

- All **business-critical systems and data** (e.g., trading platforms, client records, financial systems)
- All **internal departments** and operational processes
- **Disaster Recovery (DR) Site** and **Business Continuity** measures for data protection and operational resilience

3. Disaster Recovery and Backup Policy

- The firm maintains a **Disaster Recovery Plan (DRP)** and **Backup Policy**, which outlines the recovery strategy and backup procedures for critical data and systems.
- Backup frequency and types are outlined in the **Backup Policy** and include **daily, weekly, and monthly backups**.
- The **DRP** includes procedures for recovering from hardware/software failures, cyber-attacks, and other disruptions.
- **Data replication** to an off-site **Disaster Recovery (DR) site** is performed regularly to ensure minimal data loss and swift recovery.

4. Testing of DRP and BCP Systems

- **Disaster Recovery and Business Continuity Plan Testing Frequency:**
    - The **DRP** and **BCP systems** are tested **at least twice a year** to ensure readiness and effectiveness. These tests simulate real disaster scenarios and validate the recovery process, failover systems, and data restoration capabilities.
- **Test Reports:**
    - After each test, a **post-test report** is prepared detailing the results, issues encountered, and corrective actions taken.
    - These reports are reviewed by senior management and updated procedures are implemented as necessary.

5. Data Storage at DR Site

- The firm maintains an off-site **Disaster Recovery (DR) site** where critical data is stored to ensure that services can be resumed quickly in case of a primary site failure.
- **Data storage** at the DR site is managed with the same **security measures** and **encryption protocols** used at the primary site to protect sensitive client information.
- The DR site is regularly **monitored**, and **data replication** is performed to ensure real-time or near-real-time backup of critical systems.

6. Operational Capacity Review Report

- An **Operational Capacity Review Report** is generated monthly to evaluate the **availability**, **performance**, and **reliability** of the firm's systems and infrastructure.
- This report includes:
    - **System uptime/downtime** statistics
    - **Capacity utilization** (e.g., storage, network bandwidth, server load)
    - Any **issues** or **incidents** identified in the previous month that may impact operational continuity or the firm's ability to recover from a disaster.
- **Action Plan:**
    - Any gaps or inefficiencies identified in the report are addressed by the IT and operations teams, and corrective actions are taken to enhance system reliability and capacity.

7. Roles and Responsibilities

Role	Responsibility
Head of IT	Oversee the DRP and BCP implementation and testing.
IT Department	Manage backup systems, data replication, and recovery procedures.
Business Continuity Team	Develop and implement continuity strategies and handle testing and incident management.
Compliance Officer	Ensure DRP and BCP comply with regulatory requirements.
Senior Management	Review and approve the DRP/BCP testing schedule and reports.

8. Monitoring and Reporting

- The **Head of IT** will monitor the execution of the Disaster Recovery and Business Continuity Plan and report to senior management quarterly.
- Any **significant failures** or **delays in recovery** must be documented and presented for investigation.
- **Monthly reports** include updates on DRP and BCP testing, data replication status, and operational capacity.

9. Review and Updates

- This policy will be reviewed whenever there are significant changes in the firm's IT infrastructure, business operations, or regulatory requirements.
- The DRP and BCP will be updated based on testing results, audit findings, and lessons learned from past incidents.

BOOK KEEPING & RECORD RETENTION POLICY

1. Purpose
This policy sets out the framework for maintaining accurate financial and operational records and retaining them for the period required under applicable **laws, regulations, and industry standards** (including SECP, PSX, and FBR guidelines).

2. Scope
This policy applies to:

- All departments including Accounts, Compliance, HR, Operations, Trading, and Risk
- All physical and electronic records including emails, contracts, client documents, trade records, and financial reports
- All employees, officers, and agents of Company

3. Legal & Regulatory References

- SECP Rule Book for Brokers
- Securities Act, 2015
- Anti-Money Laundering Act, 2010
- Income Tax Ordinance, 2001 (FBR)
- Companies Act, 2017
- PSX Regulations

4. Bookkeeping Standards
4.1. Accuracy

- All financial and transactional records must be complete, accurate, and timely recorded.
- Transactions must be supported with proper documentation (e.g., invoices, contracts, vouchers).

4.2. System of Record

- Accounting and client records shall be maintained in a **centralized, secure accounting software** and/or **trading platform.**

4.3. Periodic Reconciliations

- Bank balances, client ledgers, and trade settlements must be reconciled daily by the Finance/Operations department.

5. Record Retention Periods

Record Type	**Minimum Retention Period**	**Format**
Client KYC & Account Documents	10 years after closure	Physical & Digital
Trade Confirmations & Reports	10 years	Digital
Suspicious Transaction Reports (STRs)	10 years	Confidential/Digital
Financial Statements (Audited)	10 years	Digital & Print
Tax Records & Returns (FBR)	15 years	Print & Digital
Internal Audit Reports	10 years	Digital
Board Meeting Minutes	Permanently	Print & Digital
Staff Records (HR Files)	10 years after termination	Confidential
Correspondence with SECP/PSX/FMUs	5 years	Digital & Physical
Compliance Monitoring Logs	5 years	Digital

6. Storage and Security
6.1. Physical Records

- Stored in locked cabinets with restricted access.
- Sensitive documents (e.g., client KYC, legal contracts) must be held in fire-proof cabinets.

6.2. Electronic Records

- Stored on secure, access-controlled servers.
- Daily backups must be taken and stored offsite or on encrypted cloud services.

6.3. Access Control

- Access to records is based on role-based permissions.
- Only authorized personnel (e.g., Compliance, Finance, Audit) may retrieve sensitive files.

7. Destruction of Records

- At the end of their retention period, records must be **securely destroyed**:
  - **Physical**: Shredding or incineration
  - **Digital**: Secure deletion using approved software/tools
- A **Record Disposal Register** must be maintained by the Compliance Department.

8. Responsibilities

Role	Responsibilities
Compliance Officer	Policy implementation and audit readiness
IT Department	Ensuring data backup, security, and access control
Department Heads	Ensuring records in their function are properly maintained
Employees	Accurate record entry and safeguarding of sensitive documents

9. Monitoring & Review

- Internal audits must review adherence to this policy **at least once annually**.
- Any gaps or non-compliance should be reported to senior management immediately.

10. Policy Review

This policy will be reviewed in 3 years or sooner if:

- Regulatory requirements change
- New technology or systems are implemented
- Gaps are identified through internal or external audits

CLIENT ACCEPTANCE AND CREDITWORTHINESS ASSESSMENT POLICY

1. Purpose
This policy outlines the procedures and standards for accepting new clients—both institutional and retail—and for assessing their creditworthiness. It ensures compliance with applicable regulations, promotes sound risk management, and protects the firm against financial, operational, and reputational risks.

2. Scope
This policy applies to all departments and employees involved in client onboarding, credit evaluation, account opening, and ongoing relationship management.

3. Policy Statement
- The firm will only accept clients who meet established regulatory and internal risk criteria.
- Client acceptance is subject to verification of identity, business legitimacy, and financial soundness.
- Credit limits, where applicable (e.g., margin trading), will only be extended after proper credit assessment.

4. Governance
- This policy is approved by the **Board of Directors**.
- Any changes must be reviewed and approved by the Board.
- The Compliance, Risk, and Operations departments are jointly responsible for its implementation.

5. Client Acceptance Procedures
5.1 Institutional Clients
Acceptance of institutional clients (e.g., asset managers, corporates, banks, insurance companies) requires:
- Completion of **Know Your Customer (KYC)** documentation.
- Submission of **incorporation documents**, licenses, authorized signatories list.
- Verification of **Ultimate Beneficial Owners (UBOs)** and source of funds.
- Review of **financial statements** or audited reports.
- Approval from **Senior Management or Risk Committee**, depending on exposure level.
- Assessment of **creditworthiness** based on:
    - Financial ratios (liquidity, solvency)
    - Credit rating (if available)
    - Industry and business model risk

5.2 Retail Clients
Acceptance of individual or retail clients requires:
- Completion of **KYC forms** (including risk profiling questionnaire).
- Submission of **valid identification** and proof of address.
- Verification of **source of income/funds**.
- Screening against **sanctions and PEP lists**.
- Assessment of **credit exposure**, if applicable:
    - For margin clients: review of income sources, bank statements, or brokerage history
    - Establishment of suitable **credit/margin limits** approved by the Risk Department

6. Creditworthiness Assessment
- Credit limits are set based on the client's financial capacity, investment history, and trading behavior.
- The **Risk Management Department** reviews and recommends limits for margin trading or exposure.
- Periodic reviews are conducted at least annually, or as triggered by red flags (e.g., default, excessive losses).

7. Record-Keeping
All documents and assessment records must be retained in accordance with regulatory requirements and readily available for audit or regulatory review.

8. Monitoring and Review
- Compliance will monitor adherence to this policy.
- Internal Audit will periodically test its effectiveness.
- This policy shall be reviewed in 3 years, or as required by regulatory changes or internal assessments.

9. Exceptions

Any exceptions to this policy must be documented and approved by the **Head of Risk** and the **CEO**, with notification to the Board.

CLIENT REPORTING MECHANISM POLICY

1. Purpose
To establish clear procedures for timely and accurate reporting of client transactions, account status, and statements through multiple communication channels, ensuring transparency and client satisfaction.

2. Scope
This policy applies to all client accounts serviced by the firm and covers all reporting formats including SMS alerts and an e-mail monthly, and annual reports.

3. SMS & E-Mail Alerts

- Clients shall receive **SMS alerts** and an **e-mail** immediately upon execution of any transaction (buy/sell) on their account.
- SMS and e-mail alerts may include:
    - Client name or ID (partial for security)
    - Transaction type (Buy/Sell)
    - Security name and symbol
    - Quantity and price
    - Date and time of transaction
- The IT and Client Services departments will ensure the SMS & e-mail system is operational and messages are sent without delay.

4. Monthly Reports

- **(i) Monthly Trade Activity Report:**
    - Summary of all trades executed during the month including date, security, quantity, price, and transaction value.
- **(ii) Cash Balance Report:**
    - Detailed statement of cash inflows and outflows, opening and closing balances.
- **(iii) Tax Calculation Report:**
    - Computation of withholding taxes and other applicable taxes on trades and dividends for the month.
- Monthly reports shall be compiled and emailed to clients by the **5th business day** of the following month.
- Reports are also accessible via the client's online portal.

5. Annual Reports

- **(i) Annual Accounts Statement:**
    - Comprehensive summary of account activity for the calendar year, including trades, balances, fees, and charges.
- **(ii) CDC Sub-Account Statement:**
    - Detailed statement reflecting the client's holdings in their CDC sub-account as of year-end.
- **(iii) Item-wise Ledger:**
    - Breakdown of all ledger entries including deposits, withdrawals, charges, dividends, and taxes.
- Annual reports will be sent to clients by **end of January** following the year-end.
- Clients will receive these via secure email or postal mail based on preference.

6. Roles and Responsibilities

Role	Responsibility
Client Services Team	Prepare, verify, and distribute all client reports timely
IT Department	Maintain SMS & e-mail alert systems and client portal for report access
Compliance Team	Ensure reporting accuracy and regulatory compliance
Finance Department	Provide data related to cash balances, tax calculations, and ledgers

7. Data Security and Confidentiality

- All reports and SMS & e-mail communications will be handled securely to protect client information.
- Access to client data and reports is restricted to authorized personnel only.

8. Review and Updates

- This policy shall be reviewed annually or as required to accommodate regulatory changes or improvements in reporting technology.

CLIENT SERVICING POLICY

1. Purpose
This policy outlines the framework for assigning clients to traders and managing client relationships, ensuring tailored and efficient service delivery based on client classification.

2. Scope
This policy applies to all client-facing staff, including traders, relationship managers, and client servicing teams.

3. Client Classification and Assignment

Client Type	Assignment Basis	Service Approach
Institutional Clients	Assigned to senior traders with specialized expertise in large-volume and complex transactions	Personalized service, regular portfolio reviews, dedicated relationship managers
Individual Clients	Assigned to traders based on geographical location, trading volume, or account size	Standardized service protocols with periodic check-ins and education

- The **Manager** maintains a master list of clients and assignments.
- Clients are assigned upon onboarding and reviewed quarterly for reassignment based on changing profiles or business needs.

4. Roles and Responsibilities
- **Traders:** Execute trades, provide market insights, and maintain communication as per client needs.
- **Relationship Managers:** Serve as primary contact for client queries, service requests, and escalation.
- **Client Services Team:** Monitor service levels, update client records, and coordinate between clients and traders.
- **Compliance Department:** Ensure servicing complies with regulatory and internal policies.

5. Service Standards
- Respond to client inquiries within **24 business hours**.
- Provide trade confirmations and account statements as per regulatory timelines.
- Conduct periodic client satisfaction surveys and feedback sessions.
- Handle complaints promptly and escalate unresolved issues to senior management.

6. Review and Reporting
- Client assignments and service performance are reviewed by the Services Manager.
- Reports on client satisfaction and trader performance are submitted to senior management.

7. Policy Review
This policy shall be reviewed in 3 years or as required due to changes in business strategy or regulatory requirements.

CONFIDENTIALITY AND INFORMATION BARRIER POLICY

1. Purpose
This policy ensures the **confidentiality**, **integrity**, and **protection** of all sensitive client information — including trading positions, order sizes, and strategies — and establishes effective internal **"Chinese Walls"** to prevent unauthorized access or misuse of non-public information.

2. Scope
This policy applies to all departments and employees, especially those in:

- **Trading and Dealing Desks**
- **Institutional Sales**
- **Research and Advisory**
- **Back-office and IT systems**
- **Risk and Compliance functions**

3. Core Confidentiality Controls

Control Area	Description
Client Confidentiality	All client data, including order size, direction, and holdings, is strictly confidential and must not be shared within or outside the firm except on a "need-to-know" basis.
Employee NDA Requirement	All staff must sign confidentiality agreements upon joining and during role changes.
Information Access Control	Access to client positions is restricted through system-based access rights.
Monitoring & Audit Trails	All access to client data and dealing room activity is logged and monitored by Compliance and IT Security.

4. Existence of Chinese Wall & Information Barriers
The firm has implemented **Chinese Walls** to maintain information integrity across departments. These include:

- **Physical separation** between proprietary trading, sales, research, and retail client services
- **System-based access restrictions** to prevent internal data leaks
- **Policy-based separation of duties** to avoid conflicts of interest

No employee may share non-public information across the wall without compliance clearance.

5. Monitoring Mechanism for Information Barriers
Compliance Oversight:

- Compliance monitors email logs, access logs, and order flow reports
- Random audits are conducted to test the effectiveness of internal controls

Access Logs & Alerts:

- Any unauthorized access to sensitive areas or data triggers an alert to the **Head of Compliance**

6. Restricted Access to Dealing Room

- **The dealing room is a restricted area** with physical access limited to:
    - **Head of Trading**
    - **Authorized dealers**
    - **Designated Risk personnel (view-only)**
- Entry is controlled via **access cards / biometric system**, and monitored through **CCTV** and **entry logs**

7. Access to Client Positions

- **Only the Head of Trading** and **one designated senior dealer** have access to complete client position data.
- Systems ensure that:
    - **Junior dealers and support staff cannot view** client orders or holdings.
    - **No unauthorized employee** can export or share client trading data.

Client orders are stored and transmitted through **secure, role-restricted OMS (Order Management Systems)**.

8. Institutional Trading Controls

- Institutional clients are managed by **designated senior personnel** with:
  - **Dedicated terminals**
  - **Password-protected OMS access**
  - **Encrypted communication channels**
- **Size, type, and strategy of orders remain confidential** until execution is complete.
- **Batch order masking** is used to avoid market impact and information leakage.

9. Breach Management

In case of a suspected breach:

- Immediate suspension of involved access
- Internal investigation by Compliance
- Reporting to SECP/PSX if required
- Disciplinary action (including termination) based on severity

10. Roles and Responsibilities

Role	Responsibility
Head of Trading	Ensure operational controls in dealing room
Compliance Department	Monitor and enforce information barriers
IT Security	Maintain system-based access restrictions
Risk Management	Review for unusual access or breaches

11. Review and Training

- This policy is reviewed in 3 years by the **Compliance and Risk Committees**
- Mandatory training sessions are conducted **semi-annually** for:
  - Trading and sales staff
  - IT and operations staff

CONFLICT OF INTEREST POLICY

1. Purpose
The purpose of this policy is to identify, monitor, and resolve actual, potential, or perceived conflicts of interest that may arise during the conduct of business. This is essential to uphold the integrity, transparency, and trust of clients, regulators, and stakeholders.

2. Scope
This policy applies to:

- All employees, directors, and officers
- Associated persons, including research analysts, traders, sales teams
- Related parties and business affiliates of the firm

Applicable to both **proprietary** and **client-facing activities**.

3. Definition of Conflict of Interest
A conflict of interest occurs when an individual or the firm has competing interests or obligations that may impair their ability to act in the best interest of a client or the firm.
Examples include:

- Executing proprietary trades ahead of client orders (front-running)
- Recommending a security to clients while holding a personal or proprietary position
- Receiving inducements (e.g., commissions or gifts) from third parties to influence decisions
- Dual roles in client onboarding and investment advice
- Having personal relationships with clients that influence decision-making

4. Identification & Monitoring Mechanisms
4.1. Annual Declarations
All employees and directors must submit an annual **Conflict of Interest Declaration Form**, disclosing:

- Financial interests in securities
- External directorships or business engagements
- Personal relationships that may affect objectivity

4.2. Trade Surveillance
The Compliance Department monitors:

- Employee personal trades
- Proprietary vs. client trade timing
- Cross-departmental communications (e.g., between research and trading)

4.3. Chinese Walls (Information Barriers)

- Segregation of departments (e.g., Research vs. Sales/Trading)
- Chinese Walls between UFSL and UFML, hence there are information barriers and restricted access to sensitive information (as per SECP Circular 14 of 2025 dated June 11, 2025)
- Restricted access to sensitive information
- Pre-clearance required for communication across walls

4.4. Gifts and Inducements Register
All gifts, entertainment, and other benefits received or given must be declared and recorded.

5. Conflict Resolution Mechanisms
When a conflict is identified:
5.1. Disclosure to Client
Full and timely disclosure is made to the client, enabling informed decision-making.
5.2. Withdrawal or Recusal
In cases of personal conflict, the employee must recuse themselves from the related process, deal, or decision.
5.3. Management Oversight
The Compliance Officer evaluates the materiality of the conflict. Serious conflicts are escalated to:

- Senior Management or Board of Directors

5.4. Restrictive Measures

- Blocking of certain trades
- Suspension of employee access to sensitive systems

- Divestment or restructuring of proprietary positions

6. Roles and Responsibilities

Role	Responsibility
All Employees	Declare conflicts, avoid compromising situations
Compliance Officer	Identify, assess, and monitor conflicts; maintain registers
Department Heads	Ensure team compliance with this policy
Board / Senior Management	Oversee material conflicts and approve resolution strategies

7. Record Keeping

- Conflict disclosures and resolutions shall be recorded in a **Conflict Register**, maintained by Compliance.
- Records retained for at least **5 years**.

8. Training & Awareness

- All staff shall receive annual training on identifying and managing conflicts of interest.
- New hires must undergo orientation on this policy during onboarding.

9. Breaches & Disciplinary Action

Failure to disclose or resolve a conflict of interest appropriately may result in:

- Disciplinary action (warning, suspension, or termination)
- Reporting to SECP/PSX if regulatory breaches are involved

10. Review of Policy

This policy will be reviewed **annually**, or sooner if required by regulatory changes or business restructuring.

CUSTOMER COMPLAINT MANAGEMENT POLICY

1. Purpose
To ensure that all client complaints are handled in a fair, transparent, and timely manner in compliance with **Regulation 27** of the Securities Broker Regulations, 2016.

2. Investor / Client Guide for Lodging Complaints
Clients can lodge complaints through any of the following channels:

- **Online:** Complaint form available on the company's website
- **Email:** Send directly to the designated complaints email (complaints@ufsl.com)
- **Phone:** Dedicated complaint number [Insert Number]
- **Walk-in:** By visiting our office and completing a complaint form at the reception
- **SECP Complaint Portal:** Clients may also lodge complaints on SECP's complaint portal (https://sdms.secp.gov.pk/)

All complaints must include:

- Client Name and Account Number
- Nature of the Complaint
- Relevant Dates and Supporting Documents
- Contact Information for Follow-up

3. Complaint Receipt and Acknowledgment

- Every complaint is acknowledged within **2 business days** of receipt.
- An acknowledgment reference number is issued for tracking purposes.
- Complaints received via email or portal are auto-logged in the complaint register.

4. Monitoring of Complaint Resolution

- The **Compliance Officer** maintains a central **Complaint Register** capturing all complaints, acknowledgments, actions taken, and resolution dates.
- Each complaint is assigned to a relevant department or officer for investigation and resolution.
- Complaints are resolved within **15 business days**. If more time is needed, clients are informed of the delay with reasons.
- Weekly reports are reviewed by the **Head of Compliance**.
- **Monthly complaint summary** is submitted to the CEO and Board for oversight.
- **Serious or repeated complaints** may be escalated to the **Audit Committee or BoD**.

5. Review and Compliance

- This policy is reviewed in 3 years by the Board of Directors.
- The policy is aligned with **SECP's complaint handling guidelines** and **Securities Broker Regulations**.
- The firm cooperates fully with SECP in resolving complaints referred by the Commission.

EMPLOYEE TRADING POLICY

1. Purpose
The purpose of this policy is to regulate **personal trading and investment activities** of employees, directors, and other associated persons of the firm, to:

- Prevent **conflicts of interest**
- Avoid **insider trading** or **front-running**
- Ensure compliance with **SECP**, **PSX**, and internal regulations
- Protect the integrity and reputation of the firm

2. Scope
This policy applies to:

- All **full-time and part-time employees**
- **Directors and officers**
- **Contractors, interns**, and other associated persons
- **Immediate family members** (spouse, dependent children) of the above

It covers all trading in listed **equity securities and debt instruments.**

3. Policy Requirements
3.1 General Restrictions

- Employees shall **not misuse any material non-public information (MNPI)**.
- No **front-running** of client orders is permitted.
- Trading must not **conflict with client interests** or firm strategy.
- No employee may:
    - Engage in **short-term speculative trading**
    - Trade in securities that are on the firm's **restricted list**
    - Trade during declared **blackout periods**

4. Trading and Investment Disclosures
4.1 Account Declaration
All employees must:

- Disclose all **personal trading/investment accounts** (including family accounts) at the time of joining
- Notify Compliance of any **new brokerage or trading account** within **3 working days**
- Maintain accounts only with **approved brokers**

4.2 Pre-Trade Approval (Pre-Clearance)

- Employees must obtain **written pre-clearance** from Compliance before executing any personal trade.
- Compliance will review:
    - Order book conflicts
    - Restricted list or blackout applicability

Pre-clearance is valid for **48 hours only**.

5. Trading Monitoring and Surveillance
5.1 Monitoring Mechanism

- All employees must submit quarterly **statements** of personal trading accounts.
- The **Compliance Department** conducts:
    - **post-trade surveillance**
    - Reviews for **front-running**, suspicious patterns,
    - **Random audits** of employee trading records

5.2 Exception Reporting

- Any violation or suspicious trade is escalated to:
    - Head of Compliance
    - Chief Executive Officer
    - Board Risk/Audit Committee (if material)

6. Restricted and Watch Lists

- The firm maintains a **restricted list** of securities under internal review, potential corporate deals etc.
- Employees **cannot trade** in any security on the **restricted list**.
- A **watchlist** may also be maintained for closer monitoring.

7. Trading Blackout Periods

The following blackout periods apply:

Scenario	Blackout Period
Before publication of research reports	2 trading days before and 1 day after
Before results or material announcements	7 days prior to announcement date
During proprietary strategy shift	As communicated by Compliance

Employees in sensitive roles (e.g., Research, Trading, Management) must **not trade during blackout windows**.

8. PSX Code of Conduct Acknowledgement

- All employees must **read and sign the Code of Conduct** prescribed by **Pakistan Stock Exchange (PSX)**, specifically the section relating to **employee trading practices**.
- Signed copies are maintained by **Human Resources** and **Compliance**.
- Employees must renew the acknowledgment **annually**.

9. Breach and Disciplinary Action

Violations of this policy may result in:

- **Warning or suspension**
- **Termination of employment**
- **Regulatory reporting to SECP or PSX**
- **Legal proceedings**, in case of insider trading or serious misconduct

10. Roles and Responsibilities

Role	Responsibility
Employee	Full compliance with this policy; timely disclosures
Compliance Officer	Pre-trade approvals, surveillance, and exception reporting
HR Department	Maintain signed policies and employee account declarations
CEO / BoD	Oversight and enforcement of disciplinary action if needed

11. Training and Awareness

- All employees receive **mandatory training** on employee trading rules at onboarding and **annually** thereafter.
- Training includes case studies on **conflict of interest**, **front-running etc.**

12. Policy Review

This policy is reviewed at least in 3 years or earlier if:

- Regulations change (SECP, PSX)
- Internal audit or compliance observations recommend updates
- New products or roles are introduced that impact trading restrictions

INSIDER TRADING AND MARKET ABUSE POLICY

1. Purpose
This policy is intended to prevent, detect, and report **insider trading** and other forms of **market abuse** in accordance with applicable laws and regulations, including those set by the **Securities and Exchange Commission of Pakistan (SECP)** and the **Pakistan Stock Exchange (PSX)**.

The firm is committed to maintaining the **integrity of financial markets** and ensuring that all employees and agents conduct themselves ethically and legally at all times.

2. Scope
This policy applies to:

- All **directors**, **employees**, **consultants**, and **contractors**
- All persons who have access to **confidential or price-sensitive information**
- All **trading and advisory** activities undertaken by the firm

3. Policy on Prohibition of Insider Trading
3.1 What Is Insider Trading?
Insider trading involves:

- **Buying, selling, or dealing in securities** based on **non-public, price-sensitive information (PSI)**
- **Tipping** or passing on such information to others
- **Encouraging** someone to deal in affected securities based on insider knowledge

3.2 Prohibition
It is strictly prohibited for any person associated with the firm to:

- Trade in securities while in possession of **material non-public information**
- Disclose such information to any person not authorized to receive it
- Recommend or induce others to trade based on such information

Violations may result in:

- **Termination of employment**
- **Fines, penalties, or imprisonment** under SECP/PSX laws
- Civil or criminal liability

4. Monitoring and Detection Mechanism
The firm has established a comprehensive mechanism to **monitor**, **detect**, and **investigate** potential insider trading or market abuse activities.
4.1 Monitoring Controls

Monitoring Area	Control Description
Trade Surveillance	Daily system-generated reports highlight unusual trading activity (e.g., large trades before earnings/news)
Access Logs to Price Sensitive Info	Access to internal announcements or research reports is logged and reviewed
Watch and Restricted Lists	The firm maintains internal **watchlists** and **restricted lists** of securities
Pre-Clearance of Trades (Employees)	Employees must obtain pre-clearance from Compliance before trading listed securities
Trade Blackout Periods	Trading by insiders is suspended during sensitive periods (e.g., pre-results)

4.2 Red Flag Indicators
The following trigger investigations:

- Trading before major announcements
- High volumes in illiquid stocks
- Unusual profits in personal or related accounts
- Patterned trading by employees or connected clients

5. Employee Disclosure Requirements

- All employees must disclose **trading accounts**, including those of immediate family members
- Trades in listed securities must be reported to **Compliance** within **24 hours**
- Certain designated persons (e.g., directors, analysts, traders) are subject to **trading blackout periods**

6. Reporting and Investigation

- All suspected breaches must be reported to the **Head of Compliance** or **Whistleblower Channel**
- Investigations are conducted confidentially and may involve:
    - Reviewing trade logs and communications
    - Interviewing relevant staff
    - Coordinating with **SECP** if needed

7. Training and Awareness

- Mandatory **annual training** for all employees on insider trading and market abuse
- Training records are maintained by **Human Resources** and **Compliance**

8. Record Keeping

- Trade activity logs, access logs, and investigation records are retained for a minimum of **5 years**
- Restricted and watch lists are reviewed and updated **monthly**

9. Roles and Responsibilities

Role	Responsibility
Head of Compliance	Policy implementation, monitoring, investigations
Risk Department	Surveillance and red flag detection
HR Department	Employee disclosures and training records
All Employees	Compliance with policy and reporting of violations

10. Policy Review

- The policy will be reviewed in 3 years or sooner if:
    - Regulatory requirements change
    - Material incidents occur
    - Internal audits recommend revisions

INTERNAL CODE OF CONDUCT POLICY

1. Purpose

The purpose of this Internal Code of Conduct is to ensure **high standards of integrity, transparency, professionalism, and regulatory compliance** among all employees, officers, directors, and associated persons This Code sets out the **minimum standards of behavior** expected from all staff and aims to ensure:

- Protection of clients' interests
- Prevention of conflict of interest
- Promotion of ethical behavior and compliance culture
- Fair and orderly functioning of capital markets

2. Scope

This policy applies to:

- Directors and senior management
- Front office personnel (traders, sales, dealers)
- Back office, settlement, finance, compliance, IT, and support staff
- Any other person acting on behalf of the brokerage

3. Key Principles of Conduct

All employees must:

Principle	Description
Integrity	Act honestly and with integrity in all dealings with clients, regulators, and the public
Confidentiality	Maintain confidentiality of client and firm information
Fairness	Treat all clients fairly and without discrimination
Professionalism	Conduct themselves professionally and avoid any conduct that could harm the firm's reputation
Compliance	Comply with all applicable laws, rules, and internal policies
Client First	Always prioritize the interests of the client over personal or firm interests
No Conflict of Interest	Avoid situations where personal interests conflict with duties to clients or the firm

4. Conduct Guidelines

4.1 Client Dealings

- Always act in the **best interests of the client**
- Provide accurate and timely execution of client orders
- Ensure **no front-running**, churning, or unauthorized trading

4.2 Confidentiality

- No employee shall disclose or misuse **non-public or client information**
- Maintain strict access controls to **client data, positions, and orders**

4.3 Insider Trading and Market Abuse

- Trading on **material non-public information (MNPI)** is strictly prohibited
- Refer to the firm's **Insider Trading Policy**

4.4 Personal Trading

- Employees must **disclose their trading accounts**
- Pre-clearance is required for personal trades in listed securities
- No trading is allowed in securities on the **restricted list**

4.5 Gifts and Inducements

- Employees shall not accept or offer gifts, bribes, or any form of **undue influence**
- Any gift over a nominal value (e.g., PKR 5,000) must be reported to HR

4.6 Use of Firm Resources

- Use firm systems, email, internet, and devices **only for official purposes**
- All communications and records are subject to **monitoring and audit**

5. Conflict of Interest

- Employees must **declare any actual or potential conflict** of interest
- Examples include:
    - Personal financial interest in client accounts or trades
    - Dealing with relatives as clients
    - Simultaneous employment or advisory with market participants

Conflicts must be disclosed to the **Compliance Officer** immediately.

6. Prohibited Conduct

The following are strictly prohibited:

Prohibited Action	Notes
Front-running client orders	Illegal and unethical
Misuse of client funds or securities	Breach of trust and SECP regulations
Falsification of records or data	Grounds for dismissal and legal action
Misrepresentation or misleading clients	Breach of ethical and regulatory duty
Harassment or workplace misconduct	Handled under HR & Disciplinary Policy

7. Reporting Violations (Whistleblowing)

- Employees are encouraged to report **any suspected misconduct** confidentially to:
    - **Head of Compliance**
    - **Whistleblower channel** (anonymous reporting allowed)
- Retaliation against whistleblowers is **strictly prohibited**

8. Disciplinary Action

Violations of this Code may result in disciplinary action, including:

- **Warnings**
- **Suspension or termination**
- **Regulatory reporting** to SECP/PSX
- **Legal action** where applicable

9. Training and Acknowledgement

- All employees must receive training on the **Code of Conduct** annually
- New employees must acknowledge and sign this Code within **7 days of joining**

10. Policy Review

- The Internal Code of Conduct shall be reviewed in 3 years by the **Compliance** and approved by the **Board of Directors**

INFORMATION TECHNOLOGY (IT) POLICY

1. Policy Statement
This IT Policy ensures that all information systems, digital infrastructure, and related technologies at the firm are secure, functional, and compliant with regulatory expectations. It is designed to support operational efficiency, risk management, and client service delivery.

2. Board Approval
- Amendments require formal approval and documented justification.

3. MIS Reports Generation
- The firm maintains a robust **Management Information System (MIS)** to generate critical operational and compliance reports.
- Key reports include:
    - Trade and transaction logs
    - Client account activity summaries
    - Compliance alerts and system flags
    - System uptime/downtime and usage statistics
- MIS reports are generated **daily, weekly, or monthly**, depending on operational needs and management requirements.

4. Network Connection Monitoring (Failures – Monthly Average)
- The IT department tracks **network connectivity** and logs any connection failures or disruptions.
- A **monthly failure report** is generated showing:
    - Average number of failures
    - Duration of each failure
    - Root causes and corrective actions taken
- The **monthly average** of network outages is monitored to ensure system stability and reliability for trading operations.

5. Database Management
- All client, transaction, and operational data is stored in a **secure, regularly backed-up database**.
- The database is:
    - Maintained by certified professionals
    - Subject to daily backups (local and cloud-based)
    - Monitored for integrity, access control, and redundancy
- Recovery protocols and disaster recovery systems are in place and tested quarterly.

6. Additional IT Controls (Optional Inclusions)
To further strengthen your IT governance, you may also consider incorporating:
- **Cybersecurity Framework** – Antivirus, firewall, threat detection, and incident response protocols
- **Access Controls** – Role-based access to systems and data
- **Audit Trails** – Logging of all critical system activities and user actions
- **Third-Party Vendor Monitoring** – Evaluation of outsourced tech solutions and service providers

7. Policy Review
- This policy is reviewed and updated as required to reflect changes in technology, regulation, or firm operations.

KNOW YOUR CUSTOMER (KYC) AND CLIENT DUE DILIGENCE (CDD) POLICY

1. Purpose
This policy outlines the firm's approach to KYC (Know Your Customer) and CDD (Client Due Diligence) to comply with regulatory obligations, including those of the Securities and Exchange Commission of Pakistan (SECP), Pakistan Stock Exchange (PSX), and Anti-Money Laundering (AML) regulations. It also covers the assessment and control of credit exposure to clients.

2. Scope
This policy applies to all client onboarding, monitoring, and credit-related activities for both:

- **Retail clients** (individuals), and
- **Institutional clients** (corporate and other legal entities).

3. Policy Approval

- This policy has been formally approved by the Board of Directors.
- It shall be reviewed in 3 years or upon material regulatory changes.

4. Regulatory Observations

- Compliance Department will be responsible for the oversight and response to the observations.

5. KYC/CDD Principles
5.1 Client Identification

- Obtain and verify identity using valid CNIC, NICOP, passport, or incorporation documents.
- For legal entities, verify authorized signatories, directors, and beneficial owners (UBOs).

5.2 Risk-Based Categorization
Clients are classified based on their risk profile:

- **Low Risk** (e.g., salaried individuals with stable profiles)
- **Medium Risk** (e.g., local institutions, frequent traders)
- **High Risk** (e.g., PEPs, non-resident clients, entities with complex structures)

5.3 Enhanced Due Diligence (EDD)
Applied to:

- Politically Exposed Persons (PEPs)
- High-net-worth or high-volume traders
- Clients from high-risk jurisdictions

EDD includes:

- Senior management approval
- Additional income/wealth verification
- More frequent transaction monitoring

6. Credit Limit Extension Policy
6.1 Retail Clients

- Credit (e.g., margin trading limits) is extended based on:
    - Verified source of income
    - Bank statements or financial profile
    - Trading experience and risk appetite
- Approval required from Risk Management and Compliance
- Limits are assigned as per risk tier and reviewed annually

6.2 Institutional Clients

- Credit exposure decisions based on:
    - Audited financial statements
    - Internal or external credit rating
    - Exposure limits based on capital adequacy and trading volume
- Credit proposals are submitted to and approved by the Risk Function

7. Ongoing Due Diligence

- Regular review and update of KYC records (at least annually for high-risk clients)
- Ongoing transaction monitoring for unusual or suspicious activity

- Automated or manual flagging of red flags (e.g., abnormal trading, fund transfers)

8. Reporting and Record Keeping

- All KYC/CDD documentation is securely stored in physical or electronic format.
- Retention period: Minimum 10 years after account closure or last transaction.
- Suspicious transactions are escalated to the authorities, where necessary.

9. Roles and Responsibilities

Role	Responsibility
Compliance Department	Oversight of policy implementation and training
Operations Team	Initial KYC checks and client documentation
Risk Department	Credit assessment and exposure monitoring

10. Compliance Monitoring and Review

- Internal audits will test compliance with this policy.
- The Compliance team will track and report progress on SECP/PSX observations.
- Findings will be reported to the Board Audit Committee.

11. Exceptions and Deviations

Any exceptions to this policy must:

- Be approved in writing by the CEO and Head of Compliance
- Be reported to the Board Risk or Audit Committee

LIQUIDITY MANAGEMENT POLICY

1. Purpose
This policy outlines the firm's framework for **managing liquidity risk**, ensuring that the brokerage maintains adequate cash and liquid assets to meet its financial obligations under normal and stressed market conditions. It aims to promote prudent cash flow management, protect solvency, and comply with regulatory expectations.

2. Scope
Applies to all departments involved in financial operations, proprietary trading, risk management, and treasury functions. It covers:

- Daily cash flow and liquidity monitoring
- Short-term borrowing (STB) usage
- Proprietary book funding practices
- Approved credit facilities

3. Liquidity Management Objectives

- Ensure **daily solvency and operational continuity**
- Maintain **adequate reserves** to meet client obligations, settlements, and margin calls
- Avoid reliance on **unsecured funding** or costly emergency borrowing
- Manage funding of **proprietary trading book** responsibly
- Comply with **SECP minimum capital and liquidity requirements**

4. Daily Liquidity Monitoring

- The **Finance or Treasury Department** prepares a **daily liquidity report**, which includes:
    - **Cash and bank balances**
    - **Receivables/payables**
    - **Settlement obligations**
    - **Exposure on margin clients**
    - **Utilization of overdrafts or credit lines**
- The **Chief Financial Officer (CFO)** and **Head of Risk** review the report daily.
- Exception reports are escalated to the **CEO** if utilization crosses **[e.g., 75%]** of available limits.

5. Short-Term Borrowing (STB)

- Updated daily as part of the cash flow reporting
- Monitored via bank dashboards, manual confirmations, and ERP
- Utilization is maintained within approved **internal thresholds** (e.g., not more than **80%** of total approved limits)

6. Proprietary Book Funding

- **The proprietary trading book is *not primarily funded* through short-term borrowings**.
- Prop desk investment allocations are based on:
    - **Free cash reserves**
    - **Earnings reinvestment**
    - **Dedicated capital reserves (approved annually by the Board)**

Borrowing may be used only **temporarily** to meet liquidity mismatches, and not as a long-term source for proprietary trades.

7. Liquidity Risk Triggers and Controls

Trigger/Event	Action Taken
Daily net liquidity turns negative	Trading restrictions, client payouts delayed
Large client withdrawals (> PKR 50Mn)	Emergency funding line activated
Market stress (index drop >5% in 2 days)	Liquidity buffers reviewed; exposure reduced

8. Reporting and Governance

- Weekly liquidity reports submitted to the **CEO and Investment Committee**

- Quarterly summary shared with the **Board Risk Management Committee**
- All STB arrangements are:
    - Pre-approved by the Board
    - Compliant with SECP Regulations

9. Stress Testing and Contingency Planning

- Liquidity stress tests conducted **quarterly** based on:
    - Market-wide events
    - Prop book mark-downs
    - Client margin calls
    - Funding line withdrawal scenarios
- Contingency Funding Plan (CFP) maintained and tested annually.

10. Exceptions and Violations

- Any breach of this policy must be:
    - Reported immediately to the CEO
    - Documented and presented to the **Board Audit & Risk Committee**
    - Remedied within a predefined timeline

11. Review of Policy

- This policy shall be reviewed at least in 3 years
- Updates must be approved by the **Board of Directors**

MARGIN TRADING AND MARGIN FINANCING POLICY

1. Purpose
This policy outlines the firm's approach to offering margin trading and margin financing services in compliance with applicable rules and regulations (e.g., SECP Margin Trading Regulations, PSX guidelines). It establishes procedures for client eligibility, credit limits, collateral management, margin calls, and risk controls.

2. Scope
This policy applies to all eligible clients (retail and institutional) who engage in:

- Margin Trading (MTS) – where the client buys securities partly funded by the broker
- Margin Financing (MF) – where the broker lends funds to the client for trading purposes

It applies to all staff involved in front office, risk, compliance, and operations.

3. Regulatory Framework
The policy complies with:

- SECP Margin Trading Regulations
- SECP AML/KYC Regulations
- PSX Rule Book
- Internal Risk Management Guidelines

4. Client Eligibility Criteria

- Must have a fully verified KYC/CDD profile
- Must sign a Margin Trading Agreement (as prescribed by SECP)
- Must meet the risk profile and financial capacity requirements set by the Risk Management Department

5. Margin Limits
5.1 Per Party Exposure Limits

- The total margin exposure to any single client shall not exceed the prescribed limits
- For retail clients, exposure is subject to income verification
- For institutional clients, exposure is based on credit assessment and financial review

5.2 Margin Trading Limits

- Maximum trading leverage: [1:2 or as per internal policy]
- Client must maintain a Minimum Equity Margin of [25–30%] of exposure at all times

5.3 Margin Financing Limits

- Maximum financing shall not exceed:
    - 30% of the client's approved credit line
    - Subject to the firm's capital adequacy and liquidity position
- Financing is only allowed against approved securities list (ASL)

6. Collateral Management

- Eligible securities and cash are accepted as collateral.
- Securities are haircut as per SECP-defined risk parameters.
- Only securities on the Approved Securities List (ASL) can be used for financing/trading.

7. Margin Monitoring Mechanism

- Monitoring of client margin positions
- Daily end-of-day checks to:
    - Recalculate client exposure
    - Revalue pledged collateral
    - Identify margin shortfalls
- Reports generated for:
    - Margin adequacy
    - Breach of exposure limits
    - Outstanding margin calls

8. Margin Call Mechanism

8.1 Trigger Events for Margin Call

A margin call is triggered when:

Trigger Condition	Description
Margin Shortfall	Collateral value falls below the maintenance margin requirement
Market Decline	Sharp price drop in pledged securities
Exposure Breach	Client trades beyond approved limit
Collateral Ineligibility	Collateral becomes ineligible (e.g., security removed from ASL)

8.2 Margin Call Notification

- Margin call is communicated via:
  - **Email**
  - **Trading platform notification**
- Client is required to meet the margin call within **T+1** business day.

9. Sample Margin Call Scenarios

Scenario	Action
Market drops 15% and client's margin falls to 20%	Margin call issued for shortfall
Client buys beyond approved limit using margin	Trade blocked and call issued
Security in collateral list gets suspended	Full call for replacement margin

10. Consequences of Failure to Meet Margin Call

If the client fails to meet a margin call by the due date:

- **Positions may be liquidated** partially or fully to cover exposure
- **Penalty interest** may be applied (e.g., [X]% p.a.)
- **Trading privileges may be restricted**
- **Repeated failures** may lead to **account suspension**
- **Defaulting clients** are reported to the **SECP** and/or **PSX** as required

11. Exceptions

- Any deviation from this policy must be approved by the **Head of Risk** and **CEO**
- All exceptions shall be reported to the **Board Risk Committee**

12. Review and Updates

- This policy will be reviewed in 3 years or earlier if:
  - There is a change in SECP or PSX regulations
  - There are major internal risk incidents

ONLINE TRADING FACILITY POLICY

1. Purpose
To define the firm's policy for providing a secure, real-time, and transparent **Online Trading Facility** to clients, in line with regulatory obligations and client service standards.

2. Scope
This policy applies to the firm's online trading portal and mobile application, including all functionalities made available to retail and institutional clients.

3. Real-Time Trading Interface

- The firm shall provide clients access to a **real-time online trading interface** with no perceptible time lag between price data available on the **Pakistan Stock Exchange (PSX)** and the firm's trading platform.
- Price feeds, bid/ask quotes, and order book data shall be updated on a **real-time basis**, subject to bandwidth and API conditions provided by PSX.
- The IT Department will continuously monitor latency and ensure the trading system is operating with maximum efficiency.

4. Reports and Analytical Tools Available to Clients
Clients shall have 24/7 access to the following reports through the online trading portal and mobile app:

Report Type	Description
(i) Order Book	Real-time status of all pending, executed, and cancelled orders
(ii) Trade Book	History of trades executed by the client with time, price, and quantity
(iii) Net Positions	Real-time view of client's net positions by security
(iv) Margin Report	Details of margin requirements, available margin, and exposure levels
(v) Portfolio Analysis	Current portfolio valuation, unrealized gains/losses, and asset allocation

- All reports are downloadable and can be filtered by date range, scrip, or trade type.
- Reports are updated in real-time or near real-time, depending on data source.

5. Disclosure of Commission Rates

- As required by **PSX Notice No. PSX/N-1258 dated 9th October 2019**, commission rates charged to clients shall be **clearly disclosed** on the firm's official website.
- The commission schedule must be:
    - Updated regularly
    - Easy to locate (linked from homepage or client login page)
    - Inclusive of minimum and maximum applicable charges per transaction

6. Disclosure of Broker Management Rating (BMR)

- In accordance with **Section 37 of the Securities Brokers (Licensing and Operations) Regulations, 2016**, the firm shall prominently display its **Broker Management Rating (BMR)** on its website.
- The BMR must be:
    - Visible on the homepage and client onboarding section
    - Updated upon any rating change by the credit rating agency
    - Supported with a link to the detailed rating report (if available)

7. System Availability and Support

- Online trading platforms (web and mobile) must be operational during PSX trading hours, including pre-open and post-close sessions.
- A helpdesk or live chat support must be available during trading hours to assist clients with platform issues or trade-related queries.

8. Roles and Responsibilities

Department	Responsibility
IT Department	Maintain real-time data feeds, system uptime, latency monitoring

Department	Responsibility
Client Services	Support clients using the online portal and respond to inquiries
Operations Team	Ensure timely execution and reporting of trades
Compliance Department	Verify regulatory disclosures (commission rates, BMR) on the website

9. Security and Access Controls

- Online platforms shall be secured through two-factor authentication (2FA), encrypted login credentials, and session timeout features.
- Any system breaches or anomalies must be reported to the Compliance Officer and PSX immediately.

10. Policy Review

- This policy will be reviewed upon updates to PSX regulations, technology platforms, or client service enhancements.

ORDER RECORDING POLICY

1. Purpose

To establish standardized procedures for recording client orders accurately and securely through all communication channels, ensuring transparency, compliance with regulatory requirements, and protection of client interests.

2. Scope

This policy applies to all client orders received via telephone, email, SMS, WhatsApp, or any other communication channel.

3. Order Recording Mechanism

- **Telephone Orders:**
  - All telephone calls with clients placing orders must be recorded using the firm's voice recording system.
  - Recordings shall be stored securely for a minimum of 1 **years** or as required by SECP.
  - Traders must verbally confirm the order details (security, quantity, price, and order type) during the call.
- **Email Orders:**
  - All email orders must be saved in a designated, secure folder accessible to compliance and audit teams.
  - Orders received via email are acknowledged by sending an automated or manual confirmation email.
- **SMS and WhatsApp Orders:**
  - SMS and WhatsApp orders must be logged immediately into the order management system by authorized staff.
  - Screenshots or saved chat transcripts must be archived securely.
  - Traders confirm receipt of order via the same channel or email.

4. Monitoring and Verification

- The Compliance Department shall regularly review random samples of recorded telephone calls, emails, SMS, and WhatsApp order logs to ensure accuracy and adherence to policy.
- Any discrepancies or irregularities shall be reported immediately to senior management.
- A checklist for daily monitoring will be maintained by the compliance team.

5. Order Execution and Confirmation

- Upon execution of an order, an **email confirmation** must be sent immediately to the client detailing:
  - Security name and symbol
  - Quantity
  - Price
  - Order type (buy/sell)
  - Time and date of execution
- Copies of executed order confirmations must be archived for audit purposes.

6. Archiving and Retention

- All order records including voice recordings, emails, SMS, WhatsApp messages, and order execution confirmations shall be securely archived.
- Records will be retained for a minimum as mandated by applicable regulatory requirements.
- Access to archived records is restricted to authorized personnel only.

7. Roles and Responsibilities

Role	Responsibility
Traders	Accurately record client orders, confirm details, execute orders timely
Compliance Team	Monitor order recording, conduct audits, report irregularities
IT Department	Ensure secure storage and backup of recordings and order logs
Client Services	Send order execution confirmations promptly

8. Policy Review

- This policy shall be reviewed and updated as necessary to reflect regulatory changes or operational improvements.

PROVISIONING POLICY

1. Purpose
The purpose of this policy is to establish the principles and procedures for the recognition, measurement, and reporting of provisions related to credit losses, doubtful debts, and other contingent liabilities, ensuring compliance with applicable accounting standards and regulatory requirements.

2. Scope
This policy applies to:

- All client receivables, margin loans, and financing facilities
- Operational and legal contingencies
- Other financial exposures requiring provisioning as per IFRS and SECP guidelines

3. Regulatory Framework

- **SECP Regulations** including Broker Rules and Reporting Standards
- **IFRS 9 – Financial Instruments** (Expected Credit Loss Model)
- **Companies Act, 2017**

4. Types of Provisions

Provision Type	Description
Specific Provision	Against identified doubtful debts or client margin calls overdue beyond prescribed period
General Provision	For unidentified losses based on portfolio risk assessment
Legal Provision	For probable legal claims or contingencies
Other Provisions	For expenses or liabilities expected but not yet certain

5. Provisioning Criteria
5.1. Client Receivables & Margin Loans

- A **specific provision** shall be made for receivables overdue for more than **90 days** unless recovery is certain.
- Margin loans with unsettled debit balances beyond **90 days** will be fully provided unless collateral is sufficient and realizable.
- Regular review and aging analysis to be conducted monthly.

5.2. General Provision

- A general provision of **1% to 5%** of the outstanding receivables or margin loan portfolio may be maintained to cover unidentified credit risks.
- The exact rate will be determined annually based on historical loss experience and market conditions.

5.3. Legal Provisions

- Provisions shall be recognized when a present obligation arises from past events, and it is probable that an outflow of resources will be required to settle the obligation.
- The amount shall be estimated based on legal advice and management judgment.

6. Measurement and Recognition

- Provisions must be recognized in the **financial statements** as liabilities and charged to the **profit and loss account**.
- The firm uses the **expected credit loss (ECL) model** as per IFRS 9 to estimate provisions on financial assets.
- Provisions shall be reviewed and adjusted at each reporting date.

7. Review and Write-Off

- Provisions shall be reviewed quarterly by the Finance and Risk departments.
- If a debt is deemed **irrecoverable**, management may recommend a write-off, subject to approval by senior management and audit committee.

- Write-offs shall not exceed the amount previously provided for, unless extraordinary circumstances arise.

8. Roles and Responsibilities

Role	Responsibility
Finance Department	Prepare provision calculations, maintain aging schedules, update provision accounts
Risk Management	Assess credit risk, recommend general provision rates
Compliance Officer	Ensure provisioning complies with regulatory and accounting standards
Audit Committee	Review adequacy of provisioning and recommend policy updates
Senior Management	Approve provisioning policy and significant write-offs

9. Documentation and Record Keeping

- Maintain detailed records of all provisions, recoveries, write-offs, and related correspondence.
- Documentation supporting provisioning decisions (e.g., client correspondence, legal opinions) must be retained as per regulatory requirements.

10. Policy Review

- This policy will be reviewed in 3 years or sooner if required by regulatory changes or significant business developments.

LEGAL & REGULATORY COMPLIANCE POLICY

1. Purpose
This policy establishes the framework for ensuring full compliance with all applicable **legal and regulatory requirements**, especially related to **Anti-Money Laundering (AML)** and **Combating the Financing of Terrorism (CFT)**. It aims to protect the firm from being used, intentionally or unintentionally, for money laundering or terrorist financing.

2. Scope
This policy applies to:

- All employees, agents, directors, and officers
- All business operations including client onboarding, trading, settlement, and reporting
- All products and services offered through the firm

PART I: LEGAL AND REGULATORY COMPLIANCE
3. Regulatory Framework
Shall ensure compliance with:

- SECP AML/CFT Regulations, 2020
- Anti-Money Laundering Act, 2010 (amended)
- Securities Act, 2015
- Companies Act, 2017
- PSX Rule Book
- FATF Recommendations (as adopted by Pakistan)

4. Compliance Responsibilities

Role	Responsibility
Compliance Officer	Monitor adherence to laws, file STRs/CTRs, liaison with SECP/FMUs
Senior Management	Promote a culture of compliance; approve AML/CFT controls
All Staff	Follow all applicable policies and report suspicious activity

PART II: AML & CFT POLICY
5. Objectives

- Prevent the firm from being used for money laundering or terrorist financing
- Detect and report suspicious transactions to authorities
- Maintain records and conduct due diligence in accordance with applicable laws

6. Customer Due Diligence (CDD)
6.1. Risk-Based Approach
Clients are categorized as:

- **Low Risk** – salaried individuals, government clients
- **Medium Risk** – self-employed professionals, SMEs
- **High Risk** – PEPs (Politically Exposed Persons), foreign individuals, cash-intensive businesses

6.2. Identification & Verification

- Obtain CNIC/SNIC, proof of income, bank account, and risk profile
- Verify identity using NADRA Verisys or other approved sources
- Conduct **Enhanced Due Diligence (EDD)** for high-risk clients

6.3. Ongoing Monitoring

- Regular review of account activity vs. client profile
- Automated alerts for unusual trading volumes or patterns
- Periodic KYC updates (at least every 3 years)

7. Know Your Customer (KYC) Requirements

- Mandatory at account opening

- Verify Ultimate Beneficial Owner (UBO) for legal persons
- Refuse or exit relationship if KYC is not completed

8. Reporting Obligations

8.1. Suspicious Transaction Reports (STRs)

- Filed to **Financial Monitoring Unit (FMU)** within **7 days** of detection
- Based on red flags such as inconsistent trading behavior, shell companies, etc.

8.2. Currency Transaction Reports (CTRs)

- Mandatory reporting of cash transactions (if allowed) ≥ PKR 2 million

9. Record Keeping

- Retain all KYC, CDD, STR/CTR, and transaction records as per regulatory requirements
- Records must be retrievable and auditable by SECP or FMU

10. Sanctions & Screening

- Screen all clients and transactions against:
  - UN Sanctions Lists
  - National Counter-Terrorism Authority (NACTA) Watch Lists
  - SECP/State Bank lists
- Deny services to blacklisted or sanctioned individuals/entities

11. Training and Awareness

- **Annual AML/CFT training** for all staff
- Specialized sessions for compliance, front-office, and onboarding staff
- Training records to be maintained for audit purposes

12. Independent Audit & Testing

- Internal audit to review AML/CFT compliance **annually**
- Report findings directly to the Board/CEO

13. Policy Review

This policy will be reviewed at least in 3 years, or earlier in the event of:

- Regulatory changes
- Identified compliance gaps
- Significant changes in business operations

14. Disciplinary Action

Non-compliance with this policy may result in:

- Internal disciplinary measures (warning, suspension, termination)
- Reporting to SECP or law enforcement authorities

RELATED PARTY TRANSACTIONS (RP) POLICY

1. Purpose
The purpose of this policy is to ensure that **related party transactions (RPTs)** are conducted in a **transparent**, **fair**, and **arm's length manner**, while complying with applicable laws and regulations. It establishes procedures for identifying, approving, disclosing, and monitoring transactions with related parties.

2. Scope
This policy applies to:

- All directors, key management personnel, employees, and their close family members
- Holding, subsidiary, and associated companies
- Transactions involving goods, services, assets, leases, financing, guarantees, commissions, or consultancy with related entities

3. Legal and Regulatory Framework
This policy complies with (on best effort basis):

- **Companies Act, 2017** (Sections 208–209)
- **SECP Listed Companies (Code of Corporate Governance) Regulations, 2019**
- **IFRS – IAS 24 (Related Party Disclosures)**
- **PSX Listing Regulations**

4. Definition of Related Parties
A "related party" includes but is not limited to:

- Directors and key management personnel
- Close family members of the above
- Companies where such persons have control or significant influence
- Holding, subsidiary, associate, or joint venture entities

Refer to **IAS 24** for detailed definition.

5. Identification of Related Parties

- The **Company Secretary** will maintain a regularly updated **Related Party Register**.
- All employees, directors, and officers must disclose related party relationships annually and update the firm on any changes.

6. Approval Process for Related Party Transactions

Transaction Type	Approval Required
Ordinary RPTs (in normal course & at arm's length)	**Management + Audit Committee**
Non-ordinary RPTs or above materiality threshold	**Board of Directors**
Major transactions (e.g., loans, guarantees, significant assets)	**Shareholder approval (Special Resolution)**, if required by law

6.1. Pre-Transaction Review
Before execution, each RPT must:

- Be reviewed for compliance with **arm's length** and **fair market value** principles
- Be supported by a written agreement (where appropriate)
- Be documented with valuation, benchmarking, or independent assessment (if required)

6.2. Arm's Length Standard

- Price, terms, and conditions must be comparable to those offered to or received from unrelated third parties under similar circumstances.

7. Disclosure Requirements

- All **material RPTs** shall be disclosed in:
    - **Annual Financial Statements** under IAS 24
    - **Board and Audit Committee meeting minutes**
    - **Quarterly reports and annual report** as per PSX requirements

- Disclosures must include:
    - Name of the related party
    - Nature of the relationship
    - Value and nature of the transaction
    - Justification that transaction was conducted on an arm's length basis

8. Monitoring & Review

- The **Audit Committee** shall review RPTs at least **quarterly**.
- The **Internal Audit function** (if applicable) may conduct **periodic reviews** of RPTs and their documentation.
- Any **non-compliance** or deviation shall be reported to the **Board and SECP** as required.

9. Record Keeping

The firm shall maintain:

- Register of related parties
- Documentation of each RPT (agreements, pricing basis, approvals)
- Disclosure logs for SECP and PSX filings

Records to be retained as required by applicable regulations.

10. Conflict of Interest

No employee, director, or officer involved in an RPT shall participate in the approval process for that transaction. They must **recuse themselves** and declare the conflict.

11. Training and Communication

All key staff, especially in Finance, Compliance, and Legal, must receive **training** on:

- Identification of related parties
- Approval and documentation of RPTs
- Disclosure and reporting requirements

12. Policy Review

This policy will be reviewed in 3 years by the **Audit Committee** and updated as required by:

- Changes in laws or regulations
- Internal audit findings
- Corporate restructuring or expansion

RESEARCH POLICY

1. Purpose
To establish standards and procedures for conducting, preparing, and disseminating research reports to support informed investment decisions and maintain market integrity.

2. Scope
This policy covers all research activities related to equity markets, with particular focus on KSE 100 companies, sectors, and overall market outlook.

3. Research Guidelines

- **Objectivity & Independence:** Research must be unbiased, factual, and free from conflicts of interest.
- **Accuracy & Timeliness:** Information must be accurate and delivered in a timely manner to ensure relevance.
- **Compliance:** Adhere to SECP regulations, PSX guidelines, and internal compliance requirements.
- **Confidentiality:** Protect proprietary and client-sensitive information.
- **Disclosure:** Clearly disclose any conflicts of interest or holdings in companies under research.

4. Research Dissemination Frequency & Types

Report Type	Description	Frequency
Daily Market Wrap Report	Summary of previous day's market activity and key events	Daily (Market Close)
Daily Morning Briefing Report	Pre-market outlook including macroeconomic updates and expected market movers	Daily (Before Market Open)
Daily Technical Outlook Report	Technical analysis of key indices and select stocks	Daily
Weekly Review Report	Weekly summary and analysis of market trends and sector performance	Weekly (Every Friday)
Monthly Review Report	Detailed analysis of market, sectors, and key stocks performance	Monthly (End of Month)
Sector Reports	In-depth analysis of specific sectors within KSE	As needed / Quarterly
Equity Reports	Company-specific research on KSE 100 stocks including valuation, earnings, and outlook	As needed / Quarterly
Annual Review Report	Comprehensive review of market performance, major trends, and outlook for next year	Annual (Year-End)

5. Coverage

- Focus primarily on **KSE 100 Index companies** for equity research.
- Sector coverage includes major sectors such as Banking, Energy, Technology, FMCG, and Industrials.
- Reports include both fundamental and technical perspectives where applicable.

6. Roles and Responsibilities

- **CEO:** Oversee research quality, approve dissemination, ensure compliance.
- **Research Analysts:** Conduct research, prepare reports, and maintain data accuracy.
- **Compliance Team:** Review research reports for regulatory compliance before release.
- **Distribution Team:** Ensure timely and secure dissemination of reports to clients and internal stakeholders.

7. Dissemination Channels

- Research reports are distributed via email, client portals, and internal platforms.
- Sensitive or confidential reports require secure access controls.

8. Review and Updates

- Research processes and policy to be reviewed in 3 years.
- Analysts must update research models and assumptions regularly to reflect market changes.

SEGREGATION OF CLIENT MONEY AND ASSETS POLICY

1. Purpose
To ensure the clear separation of client funds and securities from the firm's own money and assets, safeguarding client interests and complying with regulatory requirements.

2. Scope
This policy applies to all client money and assets held, processed, or managed by the firm.

3. Policy Statement
- Client money and assets shall be held separately from the firm's own funds and assets at all times.
- The firm shall maintain dedicated client bank accounts and custodial accounts to ensure no commingling occurs.
- All transactions involving client money and assets shall be recorded accurately and reconciled regularly.

4. Client Money Handling
- Client funds received for trading, settlement, or other purposes shall be deposited promptly into designated **client trust accounts**.
- Withdrawals from client accounts shall only be made upon valid client instructions or for settlement of client trades.
- The firm shall never use client funds for its operational expenses or other proprietary purposes.

5. Client Assets Handling
- Client securities shall be held in segregated CDC sub-accounts or other custodial accounts designated for client holdings only.
- The firm will ensure client assets are not used for the firm's proprietary trading or pledged as collateral for the firm's obligations.

6. Reconciliation and Reporting
- Daily reconciliation of client money accounts and monthly reconciliation of client securities accounts shall be performed by the Finance and Compliance teams.
- Any discrepancies must be investigated immediately and reported to senior management.
- Clients shall receive regular statements reflecting their segregated money and assets.

7. Compliance and Audits
- The segregation process shall comply with SECP regulations and relevant laws.
- Internal and external audits shall verify compliance with segregation requirements at least annually.

8. Roles and Responsibilities

Role	Responsibility
Finance Department	Manage client trust accounts, perform reconciliations
Compliance Department	Monitor segregation compliance, conduct audits
Operations Team	Ensure accurate processing of client transactions
Senior Management	Review reports and address issues promptly

9. Breach Reporting
- Any breach or suspected breach of client money or asset segregation must be reported immediately to the CEO and regulatory authorities as required.

10. Policy Review
- This policy shall be reviewed as required to align with regulatory changes and business practices.

SUCCESSION PLANNING POLICY

1. Policy Statement

This policy outlines the UFSL's approach to identifying and developing internal talent to ensure continuity in key leadership and critical roles. Succession planning is essential for UFSL stability, risk management, and long-term growth.

2. Purpose
The purpose of this policy is to:

- Ensure uninterrupted leadership in key roles.
- Identify and prepare potential successors.
- Support employee development and retention.
- Minimize disruption during planned or unplanned departures.

3. Scope
This policy applies to all critical and leadership positions within the UFSL, including but not limited to:

- Chief Executive Officer (CEO)
- Senior Management (e.g., CFO, COO, etc.)
- Department Heads and other key roles as identified by leadership.

4. Responsibilities

- **Board of Directors**: Oversees succession planning for executive roles.
- **Senior Management**: Identifies key positions and suitable internal successors.
- **HR Department**: Facilitates the process, maintains records, and supports training and development initiatives.
- **Employees**: Engage in development opportunities and provide input on career goals.

5. Identification of Key Positions and Successors
Key roles will be reviewed once in three years. For each role, at least one potential internal successor will be identified, along with a backup where possible. Selection is based on performance, leadership qualities, and readiness.

6. Development and Readiness
Successors will be supported through:

- Individual development plans
- Leadership training programs
- Job rotation or stretch assignments
- Mentoring and coaching

7. Review and Monitoring
Succession plans will be reviewed and updated annually or as needed due to UFSL or personnel changes. Progress of potential successors will be monitored regularly.

8. Confidentiality
All information related to succession planning will be treated as confidential and shared only with relevant stakeholders.

9. Approval and Implementation
This policy is approved by the Board of Directors and will be implemented in coordination with senior leadership.

TRADE REVIEW PROCEDURE POLICY

1. Purpose
This policy outlines the procedures and controls to review, verify, and corroborate the buying and selling of securities executed. It aims to ensure compliance with applicable laws, prevent unauthorized trades, and maintain transparency and accountability.

2. Scope
This policy applies to all trading activities executed on behalf of its clients and proprietary accounts, across all asset classes listed on the Pakistan Stock Exchange (PSX).

3. Regulatory References
- Securities Act, 2015
- PSX Rule Book
- SECP Code of Conduct for Brokerage Houses
- Anti-Market Abuse Guidelines

4. Responsibilities

Role	Responsibilities
Compliance Officer	Oversight and periodic review of all trade activities
Head of Trading	Ensures execution within client instructions and market regulations
Operations Team	Daily reconciliation and exception reporting
Internal Audit (where applicable)	Independent verification of trade review process

5. Trade Review Procedures
5.1. Pre-Trade Controls
- Verify client account status (KYC, risk profile, margin availability).
- Confirm client instructions (via recorded calls, written orders, or trade platforms).
- Ensure proper authorization for proprietary trades.

5.2. Post-Trade Review (Daily)
- **Trade Reconciliation:**
  Match trade confirmations from PSX with internal order management system.
- **Random Sampling Review:**
  At least 5–10% of daily trades are randomly selected and reviewed for:
  - Instruction authenticity
  - Price/time accuracy
  - Market manipulation red flags
- **Exception Reporting:**
  Flag and report anomalies such as:
  - Wash trades
  - Off-market price trades
  - Trades without client instruction

5.3. Weekly Oversight
- Generate weekly trade summaries.
- Compliance to review patterns for unusual volume or price behavior.
- Documentation of reviewed trades with remarks.

5.4. Monthly Review
- Internal reporting to management.
- Identify high-risk clients or trading strategies.
- Submit compliance summary to CEO or designated authority.

6. Record Keeping
All trade instructions, confirmations, reconciliations, and review logs must be retained for a minimum of **10 years** in line with SECP record-keeping guidelines. Digital backups are mandatory.

7. Breach Management
Any deviation from authorized procedures shall be:

- Reported to the Compliance Officer immediately.
- Investigated within 48 hours.
- Reported to SECP/PSX where applicable.

8. Training
All trading and operations staff shall undergo annual training on trade review procedures, regulatory compliance, and ethical trading practices.

9. Policy Review
This policy shall be reviewed in 3 years or earlier if required by regulatory changes or internal process updates.

VALUE ADDED SERVICES POLICY

1. Purpose
This policy outlines the value-added services provided by the firm to enhance client experience, promote investor education, and ensure digital accessibility and transparency through online tools and support services.

2. Scope
Applies to all departments involved in client interaction, investor education, account opening, digital content management, and technology.

3. Investor Awareness Programs

- The firm shall regularly conduct **Investor Awareness Programs** aimed at educating clients and the general public on:
    - Basics of capital markets
    - Risks and rewards of investing
    - Rights and responsibilities of investors
    - Use of trading platforms and market tools
- **Mediums for Awareness:**
    - Webinars
    - In-person workshops or seminars
    - Online tutorials and blog content
    - Social media awareness campaigns
    - Collaboration with SECP or PSX for joint sessions
- Programs shall be conducted periodically and content shall be updated based on market developments and regulatory changes.

4. Account Opening Mediums
To facilitate seamless client onboarding, the firm provides multiple account opening options:

Medium	Description
Online Portal	Fully digital account opening through firm's website
Mobile App	Account setup via the firm's secure trading app
Walk-In Service	Physical form submission at branch/office
Assisted Onboarding	Through sales agents or relationship managers

- Digital onboarding complies with SECP's e-KYC guidelines.
- Real-time status updates and client support are provided during the account opening process.

5. Functional and Accessible Website
The firm's website shall be maintained to ensure it is:

- **Functional**: All pages and tools (including account opening, research, and market data) are regularly tested and operational.
- **Accessible**: Mobile-friendly and responsive across devices; accessible to clients with disabilities where possible.
- **Updated**: Contains latest information on products, services, compliance disclosures, and contact details.
- **Secure**: Follows standard encryption protocols and user data privacy guidelines.

The IT and Marketing teams shall conduct a periodic review of website performance and usability.

6. Market Analyzer Tool
The firm shall provide a **Market Analyzer** section on the website and mobile app, displaying key market metrics:

Metric	Description
Top Traded	Stocks with highest trading volume
Top Gainers	Stocks with highest positive % price change
Top Losers	Stocks with highest negative % price change

Metric	Description
Other Details	% Change, Total Quantity, Total Value per stock

- Data is updated in **real-time** or with minimal delay (e.g., 15-second refresh).
- Users can filter data by sector, index (e.g., KSE-100), or custom watchlists.

7. Roles and Responsibilities

Department	Responsibilities
Business Development	Conduct investor awareness programs
Operations	Manage onboarding experience and support
IT & Web Team	Maintain website functionality, security, and uptime
Marketing	Ensure content accuracy and accessibility on digital platforms
Compliance	Ensure services align with SECP and PSX guidelines

8. Review and Updates

- This policy will be reviewed upon the introduction of new services or regulatory requirements.
- Suggestions for improvement may be gathered from client feedback surveys and system analytics.

WHISTLE BLOWING POLICY

1. Purpose

This policy encourages employees, clients, and stakeholders to report any unlawful, unethical, or suspicious activities without fear of retaliation. It ensures that concerns are addressed promptly, fairly, and confidentially.

2. Scope

This policy applies to:

- All employees (permanent, temporary, and contractual)
- Directors and management
- Clients and third-party stakeholders

Applicable areas include:

- Fraud, bribery, or corruption
- Insider trading or market manipulation
- Regulatory violations (SECP/PSX)
- Breach of company policies or code of ethics
- Misuse of company resources
- Harassment or discrimination

3. Principles

- **Confidentiality:** All whistleblower identities and reports will be kept strictly confidential.
- **Protection:** No retaliation, harassment, or disadvantage will be tolerated against whistleblowers.
- **Good Faith:** Reports must be made honestly. Malicious or knowingly false reports may result in disciplinary action.

4. Reporting Channels

A concern can be reported via any of the following methods:

1. **Email:**
   Send detailed reports to: **whistleblower@ufsl.com** (monitored by Internal Audit)
2. **Physical Mail:**
   Marked "Confidential" –
   Compliance Officer,
   [Head Office Address],
3. **In-person Meeting:**
   By appointment with the Compliance Officer or HR Head.

5. Procedure for Handling Reports

1. **Acknowledgement** – Report is acknowledged within **2 business days**.
2. **Preliminary Review** – Compliance Officer evaluates the issue within **5 business days**.
3. **Investigation** – If warranted, an investigation is launched. All relevant data is collected and interviews conducted.
4. **Resolution & Action** – Findings are shared with senior management or board for appropriate action.
5. **Closure** – Whistleblower is informed of the outcome (where appropriate).

6. Roles & Responsibilities

Role	Responsibility
Compliance Officer	Main point of contact; conducts initial screening and leads investigations
HR Department	Supports in employee-related matters and ensures non-retaliation
Audit Committee / Board	Oversight of serious issues and final decision-making where required

7. Retention of Records

All whistleblower complaints and investigation documents will be retained for a minimum of **5 years** in a secure and confidential manner.

8. Review of Policy

This policy shall be reviewed in 3 years by the Internal Audit Department and updated as necessary to ensure alignment with regulatory and internal requirements.