Segregation Policy

Objective: To ensure that Research Analyst (RA) activities at Stoic Wealth are conducted independently and at an arm's length from other business activities, in compliance with SEBI regulations.

1. Policy Statement

Stoic Wealth is committed to maintaining a clear and distinct separation between its Research Analyst activities and other business operations. This policy outlines the procedures to ensure that RA activities are conducted independently, without any undue influence or conflict of interest from other business activities.

2. Scope

This policy applies to all employees, directors, and business units of Stoic Wealth involved in RA activities and other business operations.

3. Key Elements

3.1 Organizational Structure

- **Separate Teams:** Establish separate teams for RA activities and other business functions to ensure independence.
- **Independent Reporting:** Ensure that the RA team reports to a different chain of command than other business units to avoid conflicts of interest.

3.2 Physical and Logical Separation

- **Office Space:** Allocate separate office spaces for RA activities to prevent undue influence and ensure confidentiality.
- **IT Systems:** Use distinct IT systems and databases for RA activities to prevent unauthorized access and ensure data integrity.

3.3 Access Controls

- **Restricted Access:** Implement access controls to restrict access to RA data and systems to

authorized personnel only.
- **Data Protection:** Ensure that RA data is protected with appropriate security measures, including encryption and secure storage.

3.4 Communication Protocols

- **Information Barriers:** Establish information barriers (Chinese Walls) to prevent the flow of sensitive information between the RA team and other business units.
- **Internal Communications:** Ensure that communications between the RA team and other business units are conducted through formal channels and documented appropriately.

3.5 Compliance and Monitoring

- **Compliance Checks:** Conduct regular compliance checks to ensure adherence to this segregation policy.
- **Internal Audits:** Perform periodic internal audits to assess the effectiveness of segregation measures and identify any potential breaches.

4. Roles and Responsibilities

4.1 Research Analyst Team

- **Independence:** Conduct all RA activities independently, free from any external influence from other business units.
- **Compliance:** Adhere to all segregation protocols and report any potential conflicts of interest to the Compliance Officer.

4.2 Other Business Units

- **Respect Boundaries:** Respect the independence of the RA team and avoid any actions that could compromise their objectivity.
- **Information Barriers:** Comply with information barrier protocols and ensure that sensitive information is not shared inappropriately.

4.3 Compliance Officer

- **Monitoring and Enforcement:** Monitor compliance with this segregation policy and enforce disciplinary measures for any breaches.

- **Training and Awareness:** Provide training to all employees on the importance of segregation and the specific protocols in place.

4.4 Senior Management

- **Oversight:** Provide oversight to ensure that segregation measures are effectively implemented and maintained.
- **Support:** Support the RA team in maintaining their independence and objectivity.

5. Training and Awareness

- **Regular Training:** Conduct regular training sessions for employees on segregation protocols and the importance of maintaining independence in RA activities.
- **Policy Communication:** Ensure that this segregation policy is communicated to all employees and included in the employee handbook.

6. Non-Compliance and Remediation

- **Incident Reporting:** Establish a clear mechanism for reporting breaches of the segregation policy.
- **Investigation and Action:** Investigate reported breaches promptly and take appropriate disciplinary actions, which may include additional training, reassignment, or termination of employment.

7. Review and Update

- **Annual Review:** Review and update this policy annually to ensure continued compliance with SEBI regulations and any changes in business operations.
- **Continuous Improvement:** Continuously improve segregation measures based on feedback, regulatory updates, and best practices.

This Segregation Policy is essential for maintaining the integrity and independence of Stoic Wealth's Research Analyst activities. All employees are expected to understand and comply with this policy to ensure that RA activities are conducted at an arm's length from other business operations.

Advertisement Policy for Compliance with SEBI Guidelines

Objective: To ensure that all advertising and promotional materials used by Stoic Wealth comply with SEBI regulations and guidelines, maintaining accuracy, transparency, and integrity in communications.

1. Policy Statement

Stoic Wealth is committed to adhering to SEBI guidelines in all advertising and promotional activities. This policy outlines the standards and procedures to ensure that advertisements are truthful, not misleading, and provide clear and accurate information to clients and the public.

2. Scope

This policy applies to all employees and third-party agents involved in the creation, approval, and dissemination of advertising and promotional materials for Stoic Wealth.

3. Key Principles

3.1 Accuracy and Truthfulness

- **Fact-Based:** Ensure that all statements in advertisements are factual, accurate, and can be substantiated.
- **No Misleading Information:** Avoid any information that is misleading, exaggerated, or deceptive.

3.2 Clarity and Transparency

- **Clear Language:** Use clear and straightforward language that is easily understood by the target audience.
- **Full Disclosure:** Disclose all relevant information, including risks, terms, and conditions, to provide a complete and transparent picture.

3.3 Compliance with SEBI Guidelines

- **SEBI Regulations:** Adhere to SEBI's advertising guidelines and regulations, including

those specified in the SEBI (Research Analysts) Regulations, 2014.
- **Legal Review:** Ensure all advertisements are reviewed by the legal and compliance teams before dissemination.

4. Advertisement Creation and Approval Process

4.1 Content Standards

- **Balanced View:** Provide a balanced view, including both potential benefits and risks associated with the investment products or services.
- **Risk Disclosures:** Clearly disclose the risks associated with the investment products or services being advertised.
- **Performance Claims:** Ensure that any claims about past performance are based on actual data and include disclaimers that past performance is not indicative of future results.

4.2 Approval Process

- **Internal Review:** All advertisements must undergo a thorough internal review process, including reviews by SEBI, marketing, compliance, and legal teams.
- **Compliance Approval:** Obtain final approval from the SEBI and Compliance Officer before any advertisement is published or disseminated.

4.3 Record Keeping

- **Documentation:** Maintain records of all advertising materials, including drafts, approvals, and final versions, for a minimum period of five years.
- **Audit Trail:** Keep an audit trail of the review and approval process, including comments and changes made during the review.

5. Prohibited Practices

5.1 Misleading Claims

- **No Guarantees:** Do not guarantee returns or make unwarranted claims about the performance of any investment product or service.
- **No Omissions:** Avoid omitting any material information that could mislead the audience.

5.2 Comparative Advertising

- **Fair Comparisons:** Ensure that any comparisons with other products or services are fair, accurate, and based on relevant and comparable data.
- **Disclosure:** Disclose the basis of the comparison and any relevant differences between the compared products or services.

5.3 Testimonials and Endorsements

- **Authenticity:** Ensure that any testimonials or endorsements used in advertisements are genuine and reflect the honest opinions of the individuals.
- **Disclosure:** Disclose any compensation or incentives provided to individuals for their testimonials or endorsements.

6. Responsibilities

6.1 Marketing Team

- **Content Creation:** Develop advertising and promotional materials that comply with this policy and SEBI guidelines.
- **Initial Review:** Conduct an initial review of all advertising content to ensure accuracy and compliance before submitting it for further review.

6.2 Compliance Team

- **Policy Enforcement:** Enforce this advertisement policy and ensure all advertising materials comply with SEBI guidelines.
- **Final Approval:** Provide the final approval for all advertisements before dissemination.

6.3 Legal Team

- **Legal Review:** Review advertising materials for compliance with legal requirements and SEBI regulations.
- **Guidance:** Provide guidance on legal and regulatory issues related to advertising.

7. Training and Awareness

7.1 Employee Training

- **Regular Training:** Conduct regular training sessions for employees involved in advertising and marketing on SEBI guidelines and the firm's advertisement policy.
- **Updates:** Keep employees informed about updates to SEBI regulations and best practices in advertising.

7.2 Compliance Updates

- **Regulatory Changes:** Monitor changes in SEBI regulations related to advertising and update the policy and training materials accordingly.
- **Policy Review:** Review and update the advertisement policy annually or more frequently if required by changes in laws or business operations.

8. Monitoring and Reporting

8.1 Internal Audits

- **Regular Audits:** Conduct regular internal audits of advertising activities to ensure compliance with SEBI regulations and this policy.
- **Audit Findings:** Document audit findings and take corrective actions to address any identified deficiencies.

8.2 Reporting Mechanisms

- **Incident Reporting:** Establish clear reporting mechanisms for employees to report any issues or breaches related to advertising practices.
- **Whistleblower Protection:** Protect whistleblowers from retaliation and ensure that reports are investigated promptly and thoroughly.

This Advertisement Policy is essential for maintaining the integrity and trustworthiness of Stoic Wealth's communications. All employees and agents involved in advertising are expected to understand and comply with this policy to ensure truthful, accurate, and compliant advertising practices.

Anti-Money Laundering (AML) Policy - For Compliance

Objective: To establish and maintain procedures to detect, prevent, and report money laundering activities in compliance with SEBI and other regulatory guidelines.

1. Policy Statement

Stoic Wealth is committed to full compliance with all applicable anti-money laundering (AML) laws and regulations. This policy outlines the procedures and responsibilities for preventing money laundering activities within the firm.

2. Scope

This policy applies to all employees, directors, and officers of Stoic Wealth, including any third parties or agents acting on behalf of the firm.

3. Key Elements

3.1 Customer Due Diligence (CDD)

- **Identification and Verification:** Obtain and verify the identity of all clients before establishing a business relationship. This includes collecting identification documents such as PAN cards, Aadhaar cards, passports, or other government-issued IDs.
- **Risk Assessment:** Assess the risk profile of clients based on factors such as the nature of the business, location, and transaction patterns. Categorize clients into high, medium, or low risk.
- **Enhanced Due Diligence (EDD):** Conduct EDD for high-risk clients, which may involve additional verification steps and obtaining more detailed information about the client's background and the source of funds.

3.2 Ongoing Monitoring

- **Transaction Monitoring:** Continuously monitor client transactions to detect unusual or suspicious activities. This includes setting thresholds for transaction amounts and types that warrant further review.
- **Record Keeping:** Maintain records of all client transactions and CDD documentation for a

minimum of five years from the date of the transaction or end of the business relationship.
- **Regular Reviews:** Periodically review and update client information and risk assessments to reflect any changes in the client's risk profile.

3.3 Reporting Suspicious Activities

- **Internal Reporting:** Employees must promptly report any suspicious activities or transactions to the AML Compliance Officer. Suspicious activities may include large cash transactions, unusual patterns of behavior, or discrepancies in provided information.
- **External Reporting:** The AML Compliance Officer is responsible for reporting suspicious transactions to the Financial Intelligence Unit - India (FIU-IND) as required by law. This includes filing Suspicious Transaction Reports (STRs) and other mandatory reports.

3.4 Training and Awareness

- **Employee Training:** Provide regular AML training to all employees to ensure they understand their responsibilities and the procedures for detecting and reporting money laundering activities. Training should cover AML laws, recognizing suspicious activities, and the firm's internal reporting procedures.
- **Ongoing Education:** Keep employees informed about updates to AML regulations and best practices through continuous education programs and regular communication.

3.5 Record Keeping and Documentation

- **Retention Period:** Maintain all AML-related records, including CDD documentation, transaction records, and internal and external reports, for at least five years.
- **Accessibility:** Ensure that records are easily accessible for review by regulatory authorities and internal auditors.

3.6 Independent Audit

- **Regular Audits:** Conduct regular independent audits of the firm's AML policies and procedures to ensure compliance with regulatory requirements and the effectiveness of the AML program.
- **Audit Reports:** Document the findings of AML audits and take corrective actions to address any identified deficiencies.

4. Responsibilities

4.1 Board of Directors

- **Oversight:** Provide oversight and ensure that the firm has an effective AML program in place.
- **Approval:** Approve the AML policy and any significant amendments.

4.2 AML Compliance Officer

- **Implementation:** Implement and maintain the AML policy and procedures.
- **Monitoring:** Monitor compliance with AML laws and regulations and conduct regular risk assessments.
- **Reporting:** Ensure timely and accurate reporting of suspicious activities to FIU-IND.

4.3 Employees

- **Adherence:** Adhere to the AML policy and report any suspicious activities to the AML Compliance Officer.
- **Training:** Participate in AML training programs and stay informed about AML responsibilities.

5. Review and Updates

- **Annual Review:** The AML policy should be reviewed and updated annually or more frequently if required by changes in laws or business operations.
- **Continuous Improvement:** Continuously improve AML practices based on feedback, audit findings, and regulatory developments.

This AML policy is integral to maintaining the integrity and reputation of Stoic Wealth. All employees are expected to understand and comply with this policy to help prevent and combat money laundering activities.

Client Onboarding Policy

Objective: To establish a standardized process for onboarding new clients, ensuring compliance with regulatory requirements, and maintaining high standards of due diligence and customer service.

1. Policy Statement

Stoic Wealth is committed to a thorough and compliant client onboarding process that ensures the legitimacy and suitability of new clients. This policy outlines the procedures and responsibilities involved in onboarding new clients.

2. Scope

This policy applies to all employees involved in client onboarding, including sales, compliance, and account management teams.

3. Key Elements

3.1 Know Your Customer (KYC)

- **Identity Verification:** Collect and verify the identity of clients using government-issued identification documents such as PAN cards, Aadhaar cards, passports, or other valid IDs.
- **Address Verification:** Obtain proof of address documents, such as utility bills, bank statements, or rental agreements, to verify the client's residence.

3.2 Client Risk Assessment

- **Risk Profiling:** Assess the risk profile of each client based on factors such as the nature of the client's business, geographical location, transaction patterns, and potential exposure to money laundering or terrorism financing.
- **Risk Categorization:** Categorize clients into high, medium, or low-risk categories to determine the level of due diligence required.

3.3 Anti-Money Laundering (AML) Compliance

- **AML Screening:** Screen clients against relevant sanctions lists, politically exposed persons (PEP) lists, and other watchlists to identify any potential AML risks.

- **Enhanced Due Diligence (EDD):** Conduct EDD for high-risk clients, which may include obtaining additional information about the client's background, source of funds, and business activities.

3.4 Client Suitability

- **Financial Information:** Gather financial information, including income, net worth, and investment objectives, to assess the suitability of products and services for the client.
- **Investment Knowledge:** Evaluate the client's knowledge and experience in financial markets to ensure appropriate product recommendations.

4. Onboarding Process

4.1 Client Application

- **Application Form:** Provide clients with a comprehensive application form to collect necessary personal, financial, and business information.
- **Documentation:** Ensure that all required documentation, including identification, address proof, and financial information, is collected and verified.

4.2 Internal Review

- **Compliance Review:** The compliance team reviews the application and supporting documents to ensure completeness and compliance with regulatory requirements.
- **Approval Process:** The client onboarding application must be approved by designated personnel, including the Compliance Officer and relevant department heads.

4.3 Account Setup

- **Account Creation:** Once approved, create the client's account in the firm's systems and assign a unique client identification number.
- **Client Communication:** Send a welcome package to the client, including account details, terms and conditions, and contact information for client support.

4.4 Ongoing Monitoring

- **Transaction Monitoring:** Continuously monitor client transactions for unusual or suspicious activities, and conduct regular reviews of high-risk clients.

- **Periodic Reviews:** Update client information and risk assessments periodically, or when there are significant changes in the client's profile or business activities.

5. Responsibilities

5.1 Sales Team

- **Initial Contact:** Make the initial contact with prospective clients and provide them with the necessary application forms and documentation requirements.
- **Assistance:** Assist clients in completing the application form and gathering required documents.

5.2 Compliance Team

- **Review and Verification:** Review and verify all client-provided information and documentation for accuracy and compliance.
- **Risk Assessment:** Conduct risk assessments and categorize clients based on their risk profile.

5.3 Account Management Team

- **Account Setup:** Set up the client's account in the firm's systems once the onboarding application is approved.
- **Client Support:** Provide ongoing support to clients and address any questions or issues related to their accounts.

5.4 Management

- **Oversight:** Provide oversight and ensure that the onboarding process is followed correctly and consistently.
- **Approval:** Approve the onboarding of new clients and ensure compliance with all regulatory requirements.

6. Training and Awareness

6.1 Employee Training

- **Mandatory Training:** Provide regular training sessions for employees on the client onboarding process, KYC requirements, AML compliance, and risk assessment.
- **Regulatory Updates:** Keep employees informed about updates to regulatory requirements and best practices in client onboarding.

6.2 Client Education

- **Information Provision:** Provide clients with information about the onboarding process, their responsibilities, and the firm's policies on KYC and AML compliance.

7. Monitoring and Reporting

7.1 Internal Audits

- **Regular Audits:** Conduct regular internal audits of the client onboarding process to ensure compliance and identify areas for improvement.
- **Audit Findings:** Document audit findings and take corrective actions to address any identified deficiencies.

7.2 Reporting Mechanisms

- **Incident Reporting:** Establish clear reporting mechanisms for employees to report any issues or breaches related to the client onboarding process.
- **Whistleblower Protection:** Protect whistleblowers from retaliation and ensure that reports are investigated promptly and thoroughly.

8. Review and Updates

8.1 Annual Review

- **Policy Review:** Review and update the client onboarding policy annually or more frequently if required by changes in laws, regulations, or business operations.
- **Continuous Improvement:** Continuously improve the onboarding process based on feedback, audit findings, and industry developments.

This Client Onboarding Policy is essential for maintaining the integrity and trustworthiness of Stoic Wealth. All employees involved in client onboarding are expected to understand and comply with this policy to ensure a thorough and compliant onboarding process.

Code of Conduct and Ethics Policy

Objective: To establish standards of ethical behavior and professional conduct for all employees, directors, and officers of Stoic Wealth.

1. Policy Statement

Stoic Wealth is committed to conducting its business with the highest standards of integrity, honesty, and ethical behavior. This policy outlines the principles and guidelines for ethical conduct that all members of the firm must adhere to.

2. Scope

This policy applies to all employees, directors, officers, and any third parties or agents acting on behalf of Stoic Wealth.

3. Key Principles

3.1 Integrity and Honesty

- **Truthfulness:** Always be truthful and transparent in all communications and business dealings.
- **Fairness:** Treat all clients, colleagues, and stakeholders fairly and without bias.
- **Accountability:** Take responsibility for your actions and decisions, and ensure that they align with the firm's ethical standards.

3.2 Professionalism

- **Competence:** Maintain the necessary skills and knowledge to perform your duties effectively. Seek continuous professional development and training.
- **Diligence:** Perform your duties with due care, attention, and professionalism. Ensure the accuracy and quality of your work.
- **Respect:** Show respect for colleagues, clients, and all individuals you interact with. Avoid any behavior that could be perceived as harassment, discrimination, or bullying.

3.3 Confidentiality

- **Client Information:** Protect the confidentiality of all client information. Do not disclose

any confidential information to unauthorized parties.
- **Firm Information:** Safeguard the firm's proprietary and confidential information. Ensure that it is not misused or improperly disclosed.

3.4 Conflicts of Interest

- **Identification:** Identify and disclose any potential conflicts of interest. Avoid situations where personal interests could conflict with professional duties.
- **Management:** Manage conflicts of interest transparently and in the best interests of clients and the firm.
- **Disclosure:** Fully disclose any conflicts of interest to clients and other relevant parties as required.

3.5 Compliance with Laws and Regulations

- **Adherence:** Comply with all applicable laws, regulations, and internal policies. Ensure that your actions do not violate any legal or regulatory requirements.
- **Reporting:** Report any legal or regulatory violations or unethical behavior to the appropriate authorities within the firm.

3.6 Fair Dealing

- **Impartiality:** Conduct all business dealings impartially and without favoritism.
- **Best Interests:** Act in the best interests of clients and ensure that recommendations and advice are based on thorough analysis and research.

3.7 Insider Trading

- **Prohibition:** Do not engage in insider trading or the misuse of material non-public information for personal gain.
- **Reporting:** Immediately report any instances of suspected insider trading or misuse of confidential information.

3.8 Gifts and Entertainment

- **Acceptance:** Do not accept gifts, entertainment, or other benefits that could influence your professional judgment or create a conflict of interest.
- **Disclosure:** Disclose any gifts or entertainment received in the course of business to the

compliance officer.

4. Responsibilities

4.1 Employees

- **Adherence:** Adhere to the principles and guidelines outlined in this policy.
- **Reporting:** Report any breaches of the code of conduct or unethical behavior to the compliance officer.
- **Continuous Improvement:** Engage in continuous learning and improvement to uphold the highest ethical standards.

4.2 Management

- **Leadership:** Lead by example and promote a culture of integrity and ethical behavior within the firm.
- **Support:** Provide support and resources to employees to help them adhere to the code of conduct and ethical standards.
- **Enforcement:** Enforce the code of conduct and take appropriate disciplinary action for any violations.

5. Implementation and Monitoring

5.1 Training

- **Mandatory Training:** Provide regular training sessions on the code of conduct and ethical behavior for all employees.
- **Updates:** Keep employees informed about updates to the code of conduct and any changes in legal or regulatory requirements.

5.2 Monitoring and Reporting

- **Regular Monitoring:** Regularly monitor adherence to the code of conduct and ethical standards through internal audits and reviews.
- **Reporting Mechanisms:** Establish clear reporting mechanisms for employees to report breaches of the code of conduct or unethical behavior.
- **Whistleblower Protection:** Protect whistleblowers from retaliation and ensure that reports

are investigated promptly and thoroughly.

6. Review and Updates

- **Annual Review:** Review and update the code of conduct and ethics policy annually or more frequently if required by changes in laws or business operations.
- **Continuous Improvement:** Continuously improve the code of conduct based on feedback, audit findings, and industry best practices.

This Code of Conduct and Ethics Policy is fundamental to maintaining the integrity and reputation of Stoic Wealth. All employees, directors, and officers are expected to understand and comply with this policy to promote a culture of ethical behavior and professional conduct.

Compliance Policy

Objective: To ensure adherence to SEBI regulations and maintain high standards of ethical conduct within Stoic Wealth. This policy includes guidelines for trading restrictions for employees and the trade approval process.

1. Policy Statement

Stoic Wealth is dedicated to maintaining compliance with all applicable SEBI regulations and internal standards of conduct. This policy outlines the procedures and responsibilities for ensuring regulatory compliance, managing employee trading activities, and enforcing the trade approval process.

2. Scope

This policy applies to all employees, directors, officers, and any third parties or agents acting on behalf of Stoic Wealth.

3. Key Elements

3.1 Regulatory Compliance

- **Adherence to Regulations:** Ensure that all business activities comply with SEBI regulations and other applicable laws.
- **Compliance Officer:** Appoint a Compliance Officer responsible for overseeing compliance with regulatory requirements and internal policies.
- **Training and Education:** Provide regular training sessions to employees on compliance-related matters and updates to SEBI regulations.

3.2 Internal Controls and Monitoring

- **Internal Audits:** Conduct regular internal audits to monitor compliance with SEBI regulations and internal policies.
- **Record Keeping:** Maintain accurate records of all transactions, client interactions, and compliance-related activities for a minimum of five years.
- **Reporting Mechanisms:** Establish clear procedures for reporting and addressing compliance breaches or concerns.

4. Employee Trading Restrictions

4.1 Personal Trading Restrictions

- **Prohibited Securities:** Employees are prohibited from trading in securities of companies that Stoic Wealth is currently covering or has recently covered in research reports.
- **Restricted List:** Maintain a restricted list of securities in which employees are not allowed to trade. Update this list regularly and communicate it to all employees.

4.2 Pre-Approval for Trades

- **Trade Approval Process:** Employees must obtain pre-approval from the Compliance Officer before executing any personal trades. This applies to all securities, including stocks, bonds, and derivatives.
- **Approval Form:** Employees must complete a trade approval form, providing details of the intended trade, including the security name, trade type (buy/sell), quantity, and rationale for the trade.
- **Review and Approval:** The Compliance Officer will review the trade request to ensure it does not conflict with any ongoing research activities or create a potential conflict of interest. Approval or denial of the trade request will be communicated to the employee promptly.

4.3 Post-Trade Reporting

- **Trade Confirmation:** Employees must submit trade confirmation details to the Compliance Officer within one business day of executing a trade.
- **Monitoring:** The Compliance Officer will regularly monitor employee trades to ensure compliance with pre-approval requirements and trading restrictions.

4.4 Holding Period Requirements

- **Mandatory Holding Period:** Employees must hold any securities purchased for a minimum period, typically 30 days, to discourage speculative trading and conflicts of interest.
- **Exceptions:** Any exceptions to the holding period requirement must be approved by the Compliance Officer and documented with a valid reason.

5. Responsibilities

5.1 Employees

- **Adherence:** Adhere to all compliance policies, trading restrictions, and the trade approval process.
- **Reporting:** Report any potential compliance breaches or concerns to the Compliance Officer promptly.
- **Training:** Participate in all mandatory compliance training sessions and stay informed about regulatory updates.

5.2 Compliance Officer

- **Oversight:** Oversee compliance with SEBI regulations and internal policies.
- **Approval Process:** Manage the trade approval process and maintain records of all trade requests and approvals.
- **Monitoring:** Regularly monitor employee trading activities and enforce compliance with trading restrictions and holding period requirements.
- **Reporting:** Report any significant compliance breaches or issues to senior management and regulatory authorities as required.

5.3 Management

- **Support:** Provide support and resources to the Compliance Officer to ensure effective implementation of the compliance policy.
- **Enforcement:** Enforce disciplinary action for any violations of compliance policies or trading restrictions.

6. Implementation and Monitoring

6.1 Training

- **Mandatory Training:** Provide regular training sessions on compliance policies, trading restrictions, and the trade approval process for all employees.
- **Updates:** Keep employees informed about updates to compliance policies and SEBI regulations.

6.2 Monitoring and Reporting

- **Regular Monitoring:** Regularly monitor adherence to compliance policies, trading restrictions, and the trade approval process through internal audits and reviews.
- **Reporting Mechanisms:** Establish clear reporting mechanisms for employees to report compliance breaches or concerns.
- **Whistleblower Protection:** Protect whistleblowers from retaliation and ensure that reports are investigated promptly and thoroughly.

7. Review and Updates

- **Annual Review:** Review and update the compliance policy annually or more frequently if required by changes in laws or business operations.
- **Continuous Improvement:** Continuously improve compliance practices based on feedback, audit findings, and regulatory developments.

This Compliance Policy is essential for maintaining the integrity and reputation of Stoic Wealth. All employees, directors, and officers are expected to understand and comply with this policy to uphold the highest standards of ethical conduct and regulatory compliance.

Conflict of Interest Policy

Objective: To identify, disclose, and manage conflicts of interest that may affect the impartiality and integrity of Stoic Wealth's business activities.

1. Policy Statement

Stoic Wealth is committed to maintaining the highest standards of integrity and professionalism. This policy aims to prevent conflicts of interest that could compromise the firm's objectivity and the trust of its clients.

2. Scope

This policy applies to all employees, directors, officers, and any third parties or agents acting on behalf of Stoic Wealth.

3. Key Elements

3.1 Identifying Conflicts of Interest

- **Personal Interests:** Identify any personal financial interests or relationships that could influence professional judgment or decision-making.
- **Client Relationships:** Recognize potential conflicts arising from relationships with clients, such as receiving gifts, favors, or preferential treatment.
- **Business Activities:** Be aware of conflicts that may arise from external business activities, including directorships, partnerships, or employment with other organizations.

3.2 Disclosure of Conflicts

- **Mandatory Disclosure:** Employees must disclose any actual or potential conflicts of interest to the Compliance Officer as soon as they arise.
- **Disclosure Form:** Complete a conflict of interest disclosure form, detailing the nature of the conflict and any relevant information.
- **Ongoing Disclosure:** Continuously monitor for potential conflicts and update disclosures as necessary.

3.3 Managing Conflicts of Interest

- **Avoidance:** Where possible, avoid situations that give rise to conflicts of interest.
- **Mitigation:** If avoidance is not possible, take steps to mitigate the conflict by implementing measures such as recusal from decision-making processes, segregation of duties, or obtaining independent oversight.
- **Client Disclosure:** Fully disclose any conflicts of interest to affected clients and seek their informed consent before proceeding with related activities.

3.4 Prohibited Activities

- **Insider Trading:** Strictly prohibit the use of material non-public information for personal gain or the gain of others.
- **Preferential Treatment:** Do not give or receive preferential treatment that could influence business decisions or compromise impartiality.
- **Personal Transactions:** Employees must not engage in personal transactions that could conflict with the interests of the firm or its clients.

4. Responsibilities

4.1 Employees

- **Adherence:** Adhere to the conflict of interest policy and disclose any actual or potential conflicts promptly.
- **Reporting:** Report any concerns or breaches of the policy to the Compliance Officer.
- **Training:** Participate in training sessions on identifying, disclosing, and managing conflicts of interest.

4.2 Compliance Officer

- **Oversight:** Oversee the implementation and enforcement of the conflict of interest policy.
- **Review Disclosures:** Review conflict of interest disclosure forms and determine appropriate actions to manage or mitigate conflicts.
- **Record Keeping:** Maintain records of all disclosed conflicts of interest and the actions taken to address them.

4.3 Management

- **Support:** Provide support and resources to the Compliance Officer to ensure effective implementation of the policy.
- **Enforcement:** Enforce disciplinary action for any violations of the conflict of interest policy.

5. Implementation and Monitoring

5.1 Training

- **Mandatory Training:** Provide regular training sessions on the conflict of interest policy for all employees.
- **Updates:** Keep employees informed about updates to the policy and best practices for managing conflicts of interest.

5.2 Monitoring and Reporting

- **Regular Monitoring:** Regularly monitor adherence to the conflict of interest policy through internal audits and reviews.
- **Reporting Mechanisms:** Establish clear reporting mechanisms for employees to report potential conflicts of interest.
- **Whistleblower Protection:** Protect whistleblowers from retaliation and ensure that reports are investigated promptly and thoroughly.

6. Review and Updates

- **Annual Review:** Review and update the conflict of interest policy annually or more frequently if required by changes in laws or business operations.
- **Continuous Improvement:** Continuously improve conflict of interest management practices based on feedback, audit findings, and regulatory developments.

This Conflict of Interest Policy is crucial for maintaining the integrity and trustworthiness of Stoic Wealth. All employees, directors, and officers are expected to understand and comply with this policy to ensure impartiality and the highest standards of ethical conduct.

Cyber Security Policy

Objective: To establish a robust framework for safeguarding Stoic Wealth's information systems and data against cyber threats, ensuring the confidentiality, integrity, and availability of information.

1. Policy Statement

Stoic Wealth is committed to protecting its information assets from all forms of cyber threats. This policy outlines the procedures and responsibilities for implementing effective cybersecurity measures.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and any third parties with access to Stoic Wealth's information systems.

3. Key Elements

3.1 Risk Management

- **Risk Assessment:** Conduct regular risk assessments to identify, evaluate, and mitigate cybersecurity risks.
- **Risk Register:** Maintain a risk register to document identified risks, their impact, likelihood, and mitigation strategies.

3.2 Access Control

- **User Authentication:** Implement strong user authentication mechanisms, including multi-factor authentication (MFA) where feasible.
- **Role-Based Access:** Restrict access to information systems based on roles and responsibilities, ensuring that users only have access to the data necessary for their job functions.
- **Account Management:** Regularly review and update user accounts and permissions, and promptly deactivate accounts of terminated employees or contractors.

3.3 Data Protection

- **Data Encryption:** Encrypt sensitive data both in transit and at rest to protect it from unauthorized access and breaches.
- **Data Backup:** Perform regular backups of critical data and ensure that backups are stored securely and tested periodically for integrity and recoverability.
- **Data Classification:** Classify data based on sensitivity and apply appropriate protection measures for each classification level.

3.4 Network Security

- **Firewall Protection:** Implement and maintain firewalls to monitor and control incoming and outgoing network traffic.
- **Intrusion Detection and Prevention:** Use intrusion detection and prevention systems (IDPS) to identify and respond to suspicious activities on the network.
- **Segmentation:** Segment the network to limit the spread of cyber threats and isolate sensitive systems.

3.5 Endpoint Security

- **Anti-Malware:** Install and regularly update anti-malware software on all endpoints to protect against viruses, spyware, and other malicious software.
- **Patching:** Ensure that all software and hardware are regularly updated with the latest security patches to address vulnerabilities.
- **Device Management:** Implement policies for managing and securing mobile devices and remote access to the corporate network.

4. Incident Response

4.1 Incident Management Plan

- **Preparation:** Develop and maintain an incident response plan that outlines the steps to be taken in the event of a cyber incident.
- **Detection and Analysis:** Establish procedures for detecting, analyzing, and reporting cybersecurity incidents.
- **Containment and Recovery:** Implement measures to contain the impact of a cyber incident and restore normal operations as quickly as possible.

4.2 Incident Reporting

- **Reporting Mechanism:** Establish a clear mechanism for reporting cyber incidents, including a dedicated incident response team and contact points.
- **Documentation:** Document all incidents, including the nature of the incident, the response actions taken, and lessons learned.

4.3 Post-Incident Review

- **Root Cause Analysis:** Conduct a thorough analysis of the root cause of each incident to prevent recurrence.
- **Continuous Improvement:** Update policies, procedures, and security measures based on lessons learned from incidents.

5. Training and Awareness

5.1 Employee Training

- **Cybersecurity Training:** Provide regular cybersecurity training to all employees to raise awareness about cyber threats and best practices for protecting information.
- **Phishing Awareness:** Conduct periodic phishing simulations to educate employees about recognizing and avoiding phishing attacks.

5.2 Awareness Campaigns

- **Regular Updates:** Keep employees informed about the latest cybersecurity threats and trends through regular communications and awareness campaigns.
- **Policy Communication:** Ensure that all employees are aware of and understand the cybersecurity policy and their responsibilities.

6. Third-Party Management

6.1 Vendor Assessment

- **Due Diligence:** Conduct thorough due diligence on third-party vendors and service providers to assess their cybersecurity practices.
- **Contracts:** Include cybersecurity requirements in contracts with third-party vendors to ensure they adhere to the firm's security standards.

6.2 Monitoring

- **Third-Party Access:** Monitor and control third-party access to the firm's information systems and data.
- **Regular Audits:** Perform regular audits and assessments of third-party vendors' compliance with cybersecurity requirements.

7. Compliance and Monitoring

7.1 Regulatory Compliance

- **Legal Requirements:** Ensure compliance with all relevant laws, regulations, and industry standards related to cybersecurity and data protection.
- **Periodic Reviews:** Regularly review and update the cybersecurity policy to reflect changes in regulatory requirements and industry best practices.

7.2 Monitoring and Auditing

- **Continuous Monitoring:** Implement continuous monitoring of the firm's information systems to detect and respond to security threats in real-time.
- **Internal Audits:** Conduct regular internal audits of the cybersecurity program to ensure effectiveness and compliance with this policy.

7.3 Reporting

- **Management Reports:** Provide regular reports to senior management on the status of the firm's cybersecurity posture, including risks, incidents, and mitigation efforts.
- **Regulatory Reporting:** Comply with any regulatory reporting requirements related to cybersecurity incidents and breaches.

This Cyber Security Policy is essential for protecting Stoic Wealth's information assets and maintaining the trust of clients and stakeholders. All employees and third parties with access to the firm's information systems are expected to understand and comply with this policy to ensure a secure and resilient cyber environment.

Fit and Proper Person Policy

Objective: To ensure that all key persons and employees of Stoic Wealth meet SEBI's "fit and proper" criteria, maintaining the integrity and trustworthiness of the firm as a capital market entity.

1. Policy Statement

Stoic Wealth is committed to ensuring that all individuals in key positions and employees meet the SEBI "fit and proper" criteria. This policy outlines the procedures for assessing and verifying the fitness and propriety of such individuals.

2. Scope

This policy applies to all key persons and employees of Stoic Wealth, including directors, senior management, and individuals holding significant influence over the firm's operations.

3. Key Elements

3.1 Fit and Proper Criteria

- **Integrity and Honesty:** Individuals must exhibit high standards of integrity and honesty.
- **Competence and Capability:** Individuals must possess the necessary skills, knowledge, and experience for their roles.
- **Financial Soundness:** Individuals must demonstrate financial soundness and stability.

3.2 Assessment Process

3.2.1 Initial Assessment

- **Background Check:** Conduct thorough background checks, including verification of educational qualifications, employment history, and references.
- **Criminal Record Check:** Verify that the individual has no criminal convictions, particularly related to financial crimes or dishonesty.
- **Regulatory History:** Check for any past regulatory violations, disciplinary actions, or involvement in financial frauds.

3.2.2 Ongoing Assessment

- **Annual Declaration:** Require key persons and employees to submit an annual declaration confirming their continued compliance with the fit and proper criteria.
- **Continuous Monitoring:** Monitor ongoing compliance with fit and proper criteria through periodic reviews and audits.

3.3 Documentation and Record-Keeping

- **Fit and Proper Records:** Maintain comprehensive records of all assessments, including background checks, declarations, and any supporting documents.
- **Confidentiality:** Ensure that all records and personal information are kept confidential and securely stored.

4. Roles and Responsibilities

4.1 Human Resources (HR)

- **Initial Screening:** Conduct initial screening and background checks for new hires.
- **Documentation:** Maintain records of all fit and proper assessments and declarations.

4.2 Compliance Team

- **Regulatory Checks:** Perform regulatory and criminal record checks.
- **Ongoing Monitoring:** Ensure continuous compliance with the fit and proper criteria through periodic reviews.

4.3 Senior Management

- **Approval:** Approve the appointment of key persons and employees based on the fit and proper assessments.
- **Oversight:** Provide oversight to ensure adherence to this policy.

5. Training and Awareness

- **Employee Training:** Conduct training sessions for employees to ensure they understand the fit and proper criteria and the importance of compliance.

- **Policy Communication:** Communicate the fit and proper person policy to all employees and key persons, emphasizing their responsibilities.

6. Non-Compliance and Remediation

- **Investigation:** Investigate any allegations or evidence of non-compliance with the fit and proper criteria.
- **Remedial Actions:** Take appropriate remedial actions, which may include additional training, reassignment, or termination of employment.

7. Review and Update

- **Annual Review:** Review and update this policy annually to ensure continued compliance with SEBI guidelines and any changes in regulatory requirements.
- **Continuous Improvement:** Continuously improve the assessment process based on feedback, regulatory updates, and best practices.

This Fit and Proper Person Policy is essential for maintaining the integrity and credibility of Stoic Wealth as a capital market entity. All key persons and employees are expected to understand and comply with this policy to ensure that the firm adheres to SEBI's fit and proper criteria.

Research Policy

Objective: To ensure that research activities conducted by Stoic Wealth adhere to SEBI's Research Analyst (RA) Regulations, 2014, and maintain the highest standards of integrity, objectivity, and professionalism.

1. Policy Statement

Stoic Wealth is committed to producing high-quality, unbiased, and transparent research. This policy outlines the standards and procedures that research analysts must follow to ensure compliance with SEBI regulations and uphold the firm's ethical standards.

2. Scope

This policy applies to all research analysts and any employees involved in the preparation, publication, and dissemination of research reports at Stoic Wealth.

3. Key Principles

3.1 Independence and Objectivity

- **Impartial Analysis:** Research analysts must ensure that their analysis and recommendations are free from bias and based solely on factual information and sound judgment.
- **No Influence:** Analysts must not be influenced by any external pressures, including those from clients, sales teams, or other departments within the firm.

3.2 Transparency and Disclosure

- **Conflict of Interest Disclosure:** Fully disclose any potential conflicts of interest, including financial interests in the subject companies, personal relationships, or other affiliations.
- **Methodology Disclosure:** Clearly explain the methodology and basis for all recommendations and ratings in research reports.

3.3 Accuracy and Reliability

- **Fact-Checking:** Verify all data and information used in research reports for accuracy and reliability.

- **Sources:** Use credible and reliable sources of information. Properly attribute all data and quotes from third-party sources.

3.4 Compliance with Regulations

- **SEBI Regulations:** Adhere to all SEBI Research Analyst Regulations, 2014, including maintaining registration, avoiding conflicts of interest, and ensuring transparency.
- **Internal Policies:** Follow internal compliance policies and procedures as outlined by the firm.

4. Research Report Preparation

4.1 Content Standards

- **Clear and Concise:** Ensure that research reports are clear, concise, and free from unnecessary jargon.
- **Balanced View:** Present a balanced view by discussing both positive and negative aspects of the subject company.
- **Risk Disclosure:** Clearly disclose all material risks associated with the subject company and any recommendations made.

4.2 Review and Approval

- **Peer Review:** Subject all research reports to a peer review process to ensure accuracy, completeness, and adherence to internal standards.
- **Compliance Approval:** Obtain approval from the Compliance Officer before the publication and dissemination of research reports.

4.3 Timeliness and Updates

- **Timely Reports:** Ensure that research reports are published in a timely manner and reflect the most current information available.
- **Follow-Up Reports:** Provide timely updates and follow-up reports as new information becomes available or as market conditions change.

5. Confidentiality and Data Protection

5.1 Client Confidentiality

- **Sensitive Information:** Protect the confidentiality of sensitive client information and do not use it for personal gain.
- **Data Security:** Implement robust data security measures to protect proprietary and confidential information.

5.2 Research Confidentiality

- **Non-Disclosure:** Do not disclose unpublished research reports or findings to unauthorized parties.
- **Controlled Access:** Ensure that access to research reports and data is restricted to authorized personnel only.

6. Training and Development

6.1 Ongoing Education

- **Regulatory Updates:** Provide regular training on SEBI regulations, internal policies, and industry best practices to all research analysts.
- **Professional Development:** Encourage continuous professional development through certifications, workshops, and industry conferences.

6.2 Ethical Standards

- **Ethics Training:** Conduct regular training sessions on ethical standards and the importance of maintaining integrity and objectivity in research.

7. Monitoring and Enforcement

7.1 Internal Audits

- **Regular Audits:** Conduct regular internal audits of research activities to ensure compliance with SEBI regulations and internal policies.
- **Audit Findings:** Document audit findings and take corrective actions to address any

identified deficiencies.

7.2 Reporting Mechanisms

- **Whistleblower Policy:** Establish a whistleblower policy that allows employees to report unethical behavior or breaches of this policy without fear of retaliation.
- **Incident Reporting:** Promptly report any breaches of SEBI regulations or internal policies to the Compliance Officer.

8. Review and Updates

8.1 Annual Review

- **Policy Review:** Review and update the research policy annually or more frequently if required by changes in laws, regulations, or business operations.
- **Continuous Improvement:** Continuously improve research practices based on feedback, audit findings, and industry developments.

This Research Policy is essential for maintaining the integrity and credibility of Stoic Wealth's research activities. All research analysts and employees involved in research are expected to understand and comply with this policy to ensure the highest standards of ethical conduct and regulatory compliance.

Grievance Redressal Process

Clients can seek clarification to their query and are further entitled to make a complaint in writing, orally or telephonically.

- An email may be sent at contact@stoicwealth.in
- Alternatively, the Investor may call on +91-9175998222
- A letter may also be written with their query/complaint and posted at the below mentioned address: A-101, 45 Paramount, Lalit Estate, Baner, Pune - 411045

The client can expect a reply within 21 days of approaching the Research Analyst. In case the client is not satisfied with our response they can lodge a grievance with SEBI at http://scores.gov.in or may also write to the office of SEBI.

After exhausting the above options for resolution of the grievance, if the investor/client is still not satisfied with the outcome, they can initiate dispute resolution through the ODR Portal: https://smartodr.in/login.

For more details about the ODR mechanism, fees, timelines etc., you may read the master circular released by SEBI titled: "Online Resolution of Disputes in the Indian Securities Market" available at the following link: https://www.sebi.gov.in/legal/master-circulars/aug-2023/online-resolution-of-disputes-in-the-indian-securities-market_75220.html

Details of Compliance Officer:

- **Name:** Mr. Saurabh Suhas Mahajan
- **Contact No.:** +91-9175998222
- **Email:** contact@stoicwealth.in