2018-06-08

Newport Wealth Management, LLC

Written Policies and

Procedures

Contents

Policy Statement

Under New Jersey regulations and rules,it is unlawful for an investment adviser registered to provide investment advice unless the adviser has adopted and implemented written policies and procedures reasonably designed to prevent violation of New Jersey regulations and rules regulations by the adviser or any of its supervised persons. The rule requires advisers to consider their fiduciary and regulatory obligations under New Jersey regulations and rules, and to formalize policies and procedures to address them. This document is provided as documentation of those policies and procedures.

Reviews of these policies and procedures are to be conducted on an annual basis at a minimum. Interim reviews may be conducted in response to significant compliance events, changes in business arrangements, and regulatory developments.

Adviser will maintain copies of all policies and procedures that are in effect or were in effect at any time during the last five years.

Chief Compliance Officer Appointment

The person herein named "Chief Compliance Officer" is stated to be competent and knowledgeable regarding the Advisers Act or applicable state rule or regulation and is empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the firm. The compliance officer has a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

Chief Compliance Officer	Date Responsibility Assumed	Annual Review Completed
Christopher Helwig, CFA, CFP®	04/24/2013	6/8/18
Supervisor	**Date Responsibility Assumed**	**Annual Review Completed**
Christopher Helwig, CFA, CFP®	04/24/2013	6/8/18

Fiduciary Statement

Background

An investment adviser, whether registered or not, has an affirmative duty to act in the best interests of its clients and to make full and fair disclosure of all material facts to the exclusion of any contrary interest. Generally, facts are "material" if a reasonable investor would consider them to be important. The duty of addressing and disclosing conflicts of interest is an ongoing process and as the nature of an adviser's business changes, so does the relationship with its clients.

Firm Statement

As an investment adviser, Newport Wealth Management, LLC (hereinafter "NWM") owes its clients specific duties as a fiduciary:

- Provide advice that is suitable for the client;
- Give full disclosure of all material facts and any potential conflicts of interest to clients and prospective clients;
- Serve with loyalty and in utmost good faith;
- Exercise reasonable care to avoid misleading a client; and
- Make all efforts to ensure best execution of transactions.

NWM seeks to protect the interest of each client and to consistently place the client's interests first and foremost in all situations. It is the belief of this investment adviser that its policies and procedures are sufficient to prevent and detect any violations of regulatory requirements as well as the firm's own policies and procedures.

Code of Ethics Statement

Background

In accordance with New Jersey regulations, Newport Wealth Management, LLC ("NWM") has adopted a code of ethics to:

- Set forth standards of conduct expected of advisory personnel (including compliance with federal securities laws);
- Safeguard material non-public information about client transactions; and
- Require "access persons" to report their personal securities transactions. In addition, the activities of an investment adviser and its personnel must comply with the broad antifraud provisions of Section 206 of the Advisers Act.

Introduction

As an investment adviser firm, we have an overarching fiduciary duty to our clients. They deserve our undivided loyalty and effort, and their interests come first. We have an obligation to uphold that fiduciary duty and see that our personnel do not take inappropriate advantage of their positions and the access to information that comes with their positions.

NWM holds their directors, officers, and employees accountable for adhering to and advocating the following general standards to the best of their knowledge and ability:

- Always place the interest of the clients first and never benefit at the expense of advisory clients;
- Always act in an honest and ethical manner, including in connection with, and the handling and avoidance of, actual or potential conflicts of interest between personal and professional relationships;
- Always maintain the confidentiality of information concerning the identity of security holdings and financial circumstances of clients;
- Fully comply with all applicable laws, rules and regulations of federal, state and local governments and other applicable regulatory agencies; and
- Proactively promote ethical and honest behavior with NWM including, without limitation, the prompt reporting of violations of, and being accountable for adherence to, this Code of Ethics.

Failure to comply with NWM's Code of Ethics may result in disciplinary action, up to and including termination of employment.

Prohibited Purchases and Sales

Insider Trading

Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. The SEC defines material by saying "Information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision." Information is nonpublic if it has not been disseminated in a manner making it available to investors generally.

NWM strictly prohibits trading personally or on the behalf of others, directly or indirectly, based on the use of material, non-public or confidential information. NWM additionally prohibits the communicating of material non-public information to others in violation of the law. Employees who are aware of the misuse of material nonpublic information should report such to the Chief Compliance Officer (CCO). This policy applies to all of NWM's employees and associated persons without exception.

Please note that SEC's position that the term "material nonpublic information" relates not only to issuers but also to the adviser's securities recommendations and client securities holdings and transactions.

Personal Securities Transactions

Preapproval No

Initial Public Offerings (IPO's)

Except in a transaction exempted by the "Exempted Transactions" section of this Code of Ethics, no access person or other employee may acquire, directly or indirectly, beneficial ownership in any securities in an Initial Public Offering ("IPO") without first obtaining approval from the CCO. Any acquisition by an access person or employee in an IPO following CCO approval shall be recorded on the appropriate firm personal trading log or other designated reporting document and placed in employees file or CCO designated compliance file.

Limited or Private Offerings

Except in a transaction exempted by the "Exempted Transactions" section of this Code of Ethics, no access person or other employee may acquire, directly or indirectly, beneficial ownership in any securities in a Limited or Private Offering without first obtaining approval from the CCO. The Adviser's CCO must obtain approval from his Supervisor.

If authorized, investment personnel are required to disclose that investment when they play a part in any client's subsequent consideration of an investment in the issuer.

Blackout Periods

There is currently no blackout policy regarding the timing of access personal trading before or after client trades are made. The CCO will follow the review procedures outlined in this manual to ensure that access persons are not front-running or profiting off of the timing of client trades.

Short-Term Trading

Securities held in client accounts may not be purchased and sold, or sold and repurchased, within 30 calendar days by investment personnel. The CCO may, for good cause shown, permit a short-term trade, but shall record the reasons and grant of permission with the records of the Code.

Miscellaneous Restrictions

Margin Accounts

Investment personnel are prohibited from purchasing securities on margin, unless pre-cleared by the CCO.

Short Sales

Investment personnel are prohibited from selling any security short that is owned by any client of the firm, except for short sales "against the box".

Blackout Periods

From time to time, representatives of NWM may buy or sell securities for themselves at or around the same time as clients. This may provide an opportunity for representatives of NWM to buy or sell securities before or after recommending securities to clients resulting in representatives profiting off the recommendations they provide to clients. Such transactions may create a conflict of interest. NWM will always transact client's transactions before its own when similar securities are being bought or sold.

Short-Term Trading

Securities held in client accounts may not be purchased and sold, or sold and repurchased, within 30 calendar days by investment personnel. The CCO may, for good cause shown, permit a short-term trade, but shall record the reasons and grant of permission with the records of the Code.

Exempted Transactions

The prohibitions of this section of this Code of Ethics shall NOT apply to:

- Purchases or sales affected in any account over which the access person has no direct or indirect influence or control.
- Purchases which are part of an automatic investment plan, including dividend reinvestment plans.
- Purchases effected upon the exercise of rights issued by an issuer pro rata to all holders of a class of its securities, to the extent such rights were acquired from such issuer, and sales of rights so acquired.
- Acquisition of securities through stock dividends, dividend reinvestments, stock splits, reverse stock splits, mergers, consolidations, spin-offs, and other similar corporate reorganizations or distributions generally applicable to all holders of the same class of securities.
- Open end investment company shares other than shares of investment companies advised by the firm or its affiliates or sub-advised by the firm.
- Certain closed-end index funds
- Unit investment trusts
- Exchange traded funds that are based on a broad-based securities index
- Futures and options on currencies or on a broad-based securities index

Prohibited Activities

Conflicts of Interest

NWM has an affirmative duty of care, loyalty, honesty, and good faith to act in the best interest of its clients. All supervised persons must refrain from engaging in any activity or having a personal interest that presents a "conflict of interest." A conflict of interest may arise if your personal interest interferes, or appears to interfere, with the interests of NWM or its clients. A conflict of interest can arise whenever you take action or have an interest that makes it difficult for you to perform your duties and responsibilities for NWM honestly, objectively and effectively.

While it is impossible to describe all of the possible circumstances under which a conflict of interest may arise, listed below are situations that most likely could result in a conflict of interest and that are prohibited under this Code of Ethics:

- Access persons may not favor the interest of one client over another client (e.g., larger accounts over smaller accounts, accounts compensated by performance fees over accounts not so compensated, accounts in which employees have made material personal investments, accounts of close friends or relatives of supervised persons). This kind of favoritism would constitute a breach of fiduciary duty; and
- Access persons are prohibited from using knowledge about pending or currently considered securities transactions for clients to profit personally, directly or indirectly, as a result of such transactions, including by purchasing or selling such securities.

Access persons are prohibited from recommending, implementing or considering any securities transaction for a client without having disclosed any material beneficial ownership, business or personal relationship, or other material interest in the issuer or its affiliates, to the CCO. If the

CCO deems the disclosed interest to present a material conflict, the investment personnel may not participate in any decision-making process regarding the securities of that issuer.

Gifts and Entertainment

Supervised persons should not accept inappropriate gifts, favors, entertainment, special accommodations, or other things of material value that could influence their decision-making or make them feel beholden to a person or firm. Similarly, supervised persons should not offer gifts, favors, entertainment or other things of value that could be viewed as overly generous or aimed at influencing decision-making or making a client feel beholden to the firm or the supervised person.

No supervised person may receive any gift, service, or other thing of more than de minimis value of from any person or entity that does business with or on behalf of the adviser. No supervised person may give or offer any gift of more than de minimis value to existing clients, prospective clients, or any entity that does business with or on behalf of the adviser without written pre-approval by the CCO. The annual receipt of gifts from the same source valued at $100.00 or less shall be considered de minimis. Additionally, the receipt of an occasional dinner, a ticket to a sporting event or the theater, or comparable entertainment also shall be considered to be of de minimis value if the person or entity providing the entertainment is present. All gifts, given and received, will be recorded in a log to be signed by the supervised person and the CCO and kept in the supervised persons file.

No supervised person may give or accept cash gifts or cash equivalents to or from a client, prospective client, or any entity that does business with or on behalf of the adviser.

Bribes and kickbacks are criminal acts, strictly prohibited by law. Supervised persons must not offer, give, solicit or receive any form of bribe or kickback

Political and Charitable Contributions

Supervised persons that may make political contributions, in cash or services, must report each such contribution to the CCO, who will compile and report thereon as required under relevant regulations. Supervised persons are prohibited from considering the adviser's current or anticipated business relationships as a factor in soliciting political or charitable donations.

Confidentiality

Supervised persons shall respect the confidentiality of information acquired in the course of their work and shall not disclose such information, except when they are authorized or legally obliged to disclose the information. They may not use confidential information acquired in the course of their work for their personal advantage. Supervised persons must keep all information about clients (including former clients) in strict confidence, including the client's identity (unless the client consents), the client's financial circumstances, the client's security holdings, and advice furnished to the client by the firm.

Service on Board of Directors

Supervised persons shall not serve on the board of directors of publicly traded companies absent prior authorization by the CCO. Any such approval may only be made if it is determined that such board service will be consistent with the interests of the clients and of NWM, and that such person serving as a director will be isolated from those making investment decisions with respect to such company by appropriate procedures. A director of a private company may be required to resign, either immediately or at the end of the current term, if the company goes public during his or her term as director.

Compliance Procedures

Compliance with Laws and Regulations

All supervised persons of NWM must comply with all applicable state, local and federal securities laws. Specifically, supervised persons are not permitted, in connection with the purchase or sale, directly or indirectly, of a security held or to be acquired by a client:

- To defraud such client in any manner;
- To mislead such client, including making any statement that omits material facts;
- To engage in any act, practice or course of conduct which operates or would operate as a fraud or deceit upon such client;
- To engage in any manipulative practice with respect to such client; or
- To engage in any manipulative practice with respect to securities, including price manipulation.

Personal Securities Transactions Procedures and Reporting

A. Pre-Clearance

For any activity where it is indicated in the Code of Ethics that pre-clearance is required, the following procedure must be followed:

1. Pre-clearance requests must be submitted by the requesting supervised person to the CCO in writing. The request must describe in detail what is being requested and any relevant information about the proposed activity.
2. The CCO will respond in writing to the request as quickly as is practical, either giving an approval or declination of the request, or requesting additional information for clarification.
3. Pre-clearance authorizations expire 48 hours after the approval, unless otherwise noted by the CCO on the written authorization response.
4. Records of all pre-clearance requests and responses will be maintained by the CCO for monitoring purposes and ensuring the Code of Ethics is followed.

B. Pre-Clearance Exemptions

The pre-clearance requirements of this section of this Code of Ethics shall not apply to:

1. Purchases or sales affected in any account over which the access person has no direct or indirect influence or control.
2. Purchases which are part of an automatic investment plan, including dividend reinvestment plans.
3. Purchases effected upon the exercise of rights issued by an issuer pro rata to all holders of a class of its securities, to the extent such rights were acquired from such issuer, and sales of rights so acquired.
4. Acquisition of covered securities through stock dividends, dividend reinvestments, stock splits, reverse stock splits, mergers, consolidations, spin-offs, and other similar corporate reorganizations or distributions generally applicable to all holders of the same class of securities.
5. Open end investment company shares other than shares of investment companies advised by the firm or its affiliates or sub-advised by the firm
6. Certain closed-end index funds.
7. Unit investment trusts.
8. Exchange traded funds that are based on a broad-based securities index.
9. Futures and options on currencies or on a broad-based securities index.

C. Reporting Requirements

1. Holdings Reports

Every access person shall, no later than ten (10) days after the person becomes an access person and annually thereafter, file an initial holdings report containing the following information:

a. The title, exchange ticker symbol or CUSIP number, type of security, number of shares and principal amount of each Reportable Security in which the access person had any direct or indirect beneficial ownership when the person becomes an access person;
b. The name of any broker, dealer or bank with whom the access person maintained an account in which any securities were held for the direct or indirect benefit of the access person; and
c. The date that the report is submitted by the access person.

2. Quarterly Reports

Every access person shall, no later than ten (10) days after the end of calendar quarter, file transaction reports containing the following information:

a. For each transaction involving a Reportable Security in which the access person had, or as a result of the transaction acquired, any direct or indirect beneficial ownership, the access person must provide the date of the transaction, the title,

exchange ticker symbol or CUSIP number, type of security, the interest rate and maturity date (if applicable), number of shares and principal amount of each involved in the transaction;

b. The nature of the transaction (e.g. purchase, sale)
c. The price of the security at which the transaction was effected
d. The name of any broker, dealer or bank with or through the transaction was effected; and
e. The date that the report is submitted by the access person.

Access persons may use duplicate brokerage confirmations and account statements in lieu of submitting quarterly transaction reports, provided that all of the required information is contained in those confirmations and statements.

3. Reporting Exemptions

The reporting requirements of this section of this Code of Ethics shall not apply to:

a. Any report with respect to securities over which the access person has no direct or indirect influence or control.
b. Transaction reports with respect to transactions effected pursuant to an automatic investment plan, including dividend reinvestment plans.
c. Transaction reports if the report would contain duplicate information contained in broker trade confirmations or account statements that the firm holds in its records so long as the firm receives the confirmations or statements no later than thirty (30) days after the end of the applicable calendar quarter.
d. Any transaction or holding report if the firm has only one access person, so long as the firm maintains records of the information otherwise required to be reported under the rule.

4. Report Confidentiality

All holdings and transaction reports will be held strictly confidential, except to the extent necessary to implement and enforce the provisions of the code or to comply with requests for information from government agencies.

Certification of Compliance

Initial Certification

The firm is required to provide all supervised persons with a copy of this Code. All supervised persons are to certify in writing that they have: (a) received a copy of this Code; (b) read and understand all provisions of this Code; and (c) agreed to comply with the terms of this Code.

Acknowledgement of Amendments

The firm must provide supervised persons with any amendments to this Code and supervised

persons must submit a written acknowledgement that they have received, read, and understood the amendments to this Code.

Annual Certification

All supervised persons must annually certify that they have read, understood, and complied with this Code of Ethics and that the supervised person has made all of the reports required by this code and has not engaged in any prohibited conduct.

The CCO shall maintain records of these certifications of compliance.

Reporting Violations

All supervised persons must report violations of the firm's Code of Ethics promptly to the CCO. If the CCO is involved in the violation or is unreachable, supervised persons may report directly to the Supervisor. All reports of violations will be treated confidentially to the extent permitted by law and investigated promptly and appropriately. Persons may report violations of the Code of Ethics on an anonymous basis. Examples of violations that must be reported are (but are not limited to):

- Noncompliance with applicable laws, rules, and regulations;
- Fraud or illegal acts involving any aspect of the firm's business;
- Material misstatements in regulatory filings, internal books and records, clients records or reports; or
- Activity that is harmful to clients, including fund shareholders; and deviations from required controls and procedures that safeguard clients and the firm.

No retribution will be taken against a person for reporting, in good faith, a violation or suspected violation of this Code of Ethics.

Retaliation against an individual who reports a violation is prohibited and constitutes a further violation of the code.

Compliance Officer Duties

Training and Education

CCO shall be responsible for training and educating supervised persons regarding this Code. Training will occur periodically as needed and all supervised persons are required to attend any training sessions or read any applicable materials.

Recordkeeping

CCO shall ensure that NWM maintains the following records in a readily accessible place:

- A copy of each code of ethics that has been in effect at any time during the past five years;
- A record of any violation of the code and any action taken as a result of such violation for five years from the end of the fiscal year in which the violation occurred;
- A record of all written acknowledgements of receipt of the code and amendments for each person who is currently, or within the past five years was a supervised person. These records must be kept for five years after the individual ceases to be a supervised person of the firm;
- Holdings and transactions reports made pursuant to the code, including any brokerage confirmation and account statements made in lieu of these report;
- A list of the names of persons who are currently, or within the past five years were, access persons;
- A record of any decision and supporting reasons for approving the acquisition of securities by access persons in initial public offerings and limited offerings for at least five years after the end of the fiscal year in which approval was granted; and
- A record of any decisions that grant employees or access persons a waiver from or exception to the code.

Annual Review

CCO shall review at least annually the adequacy of this Code of Ethics and the effectiveness of its implementation.

Sanctions

Any violations discovered by or reported to the CCO shall be reviewed and investigated promptly, and reported through the CCO to the Supervisor. Such report shall include the corrective action taken and any recommendation for disciplinary action deemed appropriate by the CCO. Such recommendation shall be based on, among other things, the severity of the infraction, whether it is a first or repeat offense, and whether it is part of a pattern of disregard for the letter and intent of this Code of Ethics. Upon recommendation of the CCO, the Supervisor may impose such sanctions for violation of this Code of Ethics as it deems appropriate, including, but not limited to:

- letter of censure;
- Suspension or termination of employment;
- Reversal of a securities trade at the violator's expense and risk, including disgorgement of any profit; and
- In serious cases, referral to law enforcement or regulatory authorities.

Definitions

1. "**Access Person**" includes any supervised person who has access to nonpublic information regarding any clients' purchase or sale of securities, or nonpublic information regarding the portfolio holdings of any fund the adviser or its control affiliates manage; or is involved in making securities recommendations to clients, or has access to such recommendations that are nonpublic. All of the firm's directors, officers, and partners are presumed to be access persons.
2. "**Act**" means Investment Advisers Act of 1940.
3. "**Adviser**" means NWM.

4. A "**Covered Security"** is "being considered for purchase or sale" when a recommendation to purchase or sell the Covered Security has been made and communicated and, with respect to the person making the recommendation, when such person seriously considers making such a recommendation.
5. "**Beneficial ownership**" shall be interpreted in the same manner as it would be under Rule 16a-1(a)(2) under the Securities Exchange Act of 1934 in determining whether a person is the beneficial owner of a security for purposes as such Act and the rules and regulations promulgated thereunder.
6. "**CCO**" means Chief Compliance Officer per rule 206(4)-7 of the Investment Advisers Act of 1940.
7. "**Conflict of Interest**": for the purposes of this Code of Ethics, a "conflict of interest" will be deemed to be present when an individual's private interest interferes in anyway, or even appears to interfere, with the interests of the Adviser as a whole.
8. "**Covered Security**" means any stock, bond, future, investment contract or any other instrument that is considered a "security" under the Act. Additionally, it includes options on securities, on indexes, and on currencies; all kinds of limited partnerships; foreign unit trusts and foreign mutual funds; and private investment funds, hedge funds, and investment clubs.
9. "**Covered Security**" does not include direct obligations of the U.S. government; bankers' acceptances, bank certificates of deposit, commercial paper, and high quality short-term debt obligations, including repurchase agreements; shares issued by money market funds; shares of open-end mutual funds that are not advised or sub-advised by the Adviser; and shares issued by unit investment trusts that are invested exclusively in one or more open-end funds, none of which are funds advised or sub-advised by the Adviser.
10. "**Initial Public Offering**" means an offering of securities registered under the Securities Act of 1933, the issuer of which, immediately before the registration, was not subject to the reporting requirements of Section 13 or Section 15(d) of the Securities Exchange Act of 1934.
11. "**Investment personnel**" means: (i) any employee of the Adviser or of any company in a control relationship to the Adviser who, in connection with his or her regular functions or duties, makes or participates in making recommendations regarding the purchase or sale of securities for clients.
12. "**Limited Offering**" means an offering that is exempt from registration under the Securities Act of 1933 pursuant to Section 4(2) or Section 4(6) thereof or pursuant to Rule 504, Rule 505 or Rule 506 thereunder.
13. "**Purchase or sale of a Covered Security**" includes, among other things, the writing of an option to purchase or sell a Covered Security.
14. "**Reportable security**" is as defined by Rule 204A-1 of the Act. For more clarification, please see this no-action letter, which spells out the Code of Ethics requirements in layman's terms: http://www.sec.gov/divisions/investment/noaction/ncs113005.htm.
15. "**Supervised Persons**" means directors, officers, and partners of the adviser (or other persons occupying a similar status or performing similar functions); employees of the adviser; and any other person who provides advice on behalf of the adviser and is subject to the adviser's supervision and control.

Privacy Policy & Information Security

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed once annually. The CCO will document the date the PPS was mailed to each client for each year. NWM collects nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us or others; and
- Information we receive from a consumer reporting agency.

We do not disclose any nonpublic personal information about you to anyone, except as permitted by law.

If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

NWM restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. NWM maintains physical, electronic, and procedural safeguards to guard your nonpublic personal information.

The following employees will manage nonpublic information: Christopher Helwig, CFA, CFP®
The following systems may be vulnerable to a breach of your nonpublic information: Custodian Website, Client Relationship Management ("CRM") system.

To mitigate a possible breach of the private information NWM will encrypt all data that individuals have access to or use password sensitive documents. The system will be tested and monitored at least annually.

NWM has taken extensive measures to safeguard the privacy and integrity of the information that it gathers, stores, and archives during its normal business practices. Computer security measures have been instituted where applicable including passwords, backups, and encryption. All employees are informed and instructed on various security measures including the non-discussion and/or sharing of client information, always removing client files from desktops or working areas that cannot be locked or secured, and proper storage of client securities files in locked files or other secured location. NWM uses various methods to store and archive client files and other information. All third party services or contractors used have been made aware of the importance NWM places on both firm and client information security. In addition to electronic and personnel measures NWM has implemented reasonable physical security measures at our home office location, and encouraged all remote locations, if any, to do the same to prevent unauthorized access to our facilities.

Social Networking Policy

The following is a listing of Social Media sites included in the SEC's letter to advisers as part of their Social Media Sweep which was announced in February 2011. This list is not intended to be all encompassing as new sites are added almost daily and posts to sites not listed here should not be considered as "safe havens" from the regulatory requirements of Social Media Usage.

Social Media Sites: 1)Facebook; 2) Twitter, including, without limitation, AdvisorTweets.com; 3) LinkedIn; 4) LinkedFa; 5) YouTube; 6) Flickr; 7) MySpace; 8) Digg; 9) Reddit; 10) RSS Feeds; and 11) Blogs and micro-blogs

The SEC requested the following documents for their sweep:

1. *All documents concerning any communications made by or received by [Adviser] on any social media website, including, without limitation, snapshots of documents sufficient to identify adviser's involvement with or usage of social media websites.*
2. *All documents concerning adviser's policies and procedures related to the use of social media web sites by adviser, including, without limitation:*
    a. *All policies and procedures concerning any communication posted on any social media website by adviser;*
    b. *All policies and procedures concerning any prospective communications to be posted on any social media website by adviser; and*
    c. *All policies and procedures concerning any ongoing monitoring or review process related to communications posted on any social media website by adviser;*
3. *All documents concerning adviser's policies and procedures concerning a third party's use of any social media website maintained by adviser, including, without limitation:*
    a. *All policies and procedures concerning any communication posted by a third party, including, without limitation, actual or prospective clients of adviser, on any social media website maintained by adviser;*
    b. *All policies and procedures concerning any approval processes for prospective communications to be posted by a third party, including, without limitation, actual or prospective clients of adviser, on any social media website maintained by adviser; and*
    c. *All policies and procedures concerning any ongoing monitoring or review processes related to communications posted by a third party, including, without limitation, actual or prospective clients of adviser, on any social media website maintained by adviser;*
4. *All documents concerning adviser's policies and procedures related to the use of social media websites by adviser's personnel for personal, non-business related matters;*
5. *All documents concerning adviser's personnel training and education related to the use of social media websites by Adviser, whether for personal, non-business related, or business related matters;*
6. *All documents concerning any informal or formal disciplinary action of [Adviser]'s personnel related to the use of social media for personal, non-business related, or business related reasons; and*

7. *All documents concerning NWM's record retention policies and procedures concerning the involvement with or usage of, whether for personal, non-business related, or business related matters, any social media website maintained by adviser by:*
   a. adviser;
   b. adviser's personnel; or
   c. any third party.

Social Network Website Listing (non-exclusive): 1)Facebook; 2) Twitter, including, without limitation, AdvisorTweets.com; 3) LinkedIn; 4) LinkedFa; 5) YouTube; 6) Flickr; 7) MySpace; 8) Digg; 9) Reddit; 10) RSS Feeds and 11) Blogs and micro-blogs

NWM has adopted the following policies and procedures concerning the usage of social media websites by its advisers and/or supervised persons:

1) All social media site usage is considered correspondence and/or advertising by NWM;
2) All advisers and/or supervised persons are required to notify the Chief Compliance Officer (CCO) of their intention to utilize social media sites PRIOR TO USAGE;
3) All usage and posting to these sites must be monitored and approved by the firm's CCO.
4) NWM's books and records policies on correspondence and advertising, require that, as correspondence and/or advertising, all social media usage and posts must be retained and archived;
5) Therefore any person wishing to utilize social media will need to obtain the services of an "archiving service provider" who will be responsible for providing the CCO with archived copies (or access to archived copies) of all usage and/or postings. This provider must be approved by the CCO;
6) Failure to follow NWM's policies and procedures by any adviser and/or supervised person may subject this individual to various sanctions, fines, and possibly termination by the firm.

These policies or procedures should be added to NWM's Policies and Procedures manual and every supervised person should acknowledge and sign off on their reading and understanding of these policies.

Anti-Money Laundering (AML) Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Anti-Money Laundering Program Compliance Officer Appointment

The person herein named "Anti-Money Laundering Program Compliance Officer" has full responsibility for the firm's AML program. This person is qualified by experience, knowledge and training. The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations and overseeing communication and training for employees. The AML Compliance Officer will also ensure that proper AML records are kept as required by law. When warranted, the AML Compliance Officer will ensure Suspicious Activity Reports (SAR-SFs) are filed.

AML Compliance Officer	Date Responsibility Assumed	Annual Review Completed
Christopher Helwig, CFA, CFP®	04/24/2013	6/8/18
Supervisor	**Date Responsibility Assumed**	**Annual Review Completed**
Christopher Helwig, CFA, CFP®	04/24/2013	6/8/18

Upon passage of any requirements by the Financial Crimes Enforcement Network (FinCEN), the SEC, or any state governing body (such as the state securities board), the firm will provide contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. If so required, the firm will promptly notify of any change to this information.

Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

FinCEN Requests under PATRIOT Act Section 314

Under Treasury's regulations, we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, (or if you don't have e-mail,) by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of Section 314 of the PATRIOT Act.

Checking the Office of Foreign Assets Control ("OFAC") List

If so required by law, before opening an account, and on an ongoing basis, we will check to ensure that a customer does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) (See the OFAC Web Site at http://www.treas.gov/ofac, which is also available through an automated search tool on

http://apps.finra.org/RulesRegulation/OFAC/1/Default.aspx), and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

Customer Identification and Verification

Prior to opening an account, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical location (for a person other than an individual); an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons). In the event that a customer has applied for, but has not received, a taxpayer identification number, we will attempt to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

When opening an account for a foreign business or enterprise that does not have and identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

Clients Who Refuse To Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our clients by using risk-based procedures to verify and document the accuracy of the information we get about our clients. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain. We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and social security number.

Appropriate documents for verifying the identity of clients include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity. We will use the following non-documentary methods of verifying identity:

- Contacting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will use non-documentary methods of verification in the following situations: (1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) when the firm is unfamiliar with the documents the customer presents for identification verification; (3) when the customer and firm do not have face-to-face contact; and (4) when there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with the firm's AML compliance officer, file a SAR-SF in accordance with applicable law and regulation.

Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (A) not open an account; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) close an account after attempts to verify customer's identity fail; and (D) file a SAR-SF if required by applicable law and regulation.

Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will maintain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

Monitoring Accounts for Suspicious Activity

We will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified below. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The AML Compliance Officer or his or her designee will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-SF are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed.

Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: we discover that a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contacts we will use are: Financial Institutions Hotline (1-866-556-3974) and our local U.S. Attorney's Office: (973)-645-2700; local FBI Office: (973) 792-3000; and our local SEC office: (212) 336-1100.

Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents;
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy;
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets;
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs;
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity;
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry;
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash;
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government

reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds;

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF;
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity;
- The customer's account shows numerous currency or cashier's check transactions aggregating to significant sums;
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose;
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven;
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose;
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose;
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account;
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose;
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements;
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.);
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions;
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose; or
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

Responding to Red Flags and Suspicious Activity

When a member of the firm detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third-party sources, contacting the government or filing a Form SAR-SF.

Suspicious Transactions and BSA Reporting

Filing a Form SAR-SF

If required by law, we will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) $5,000 or more of funds or assets where we know, suspect, or have reason to suspect: 1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation, 2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations, 3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the government immediately (See above for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or a Self-Regulatory Organization (SRO) may also be reported promptly to the local U.S. Attorney, as appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO.

All SAR-SFs will be periodically reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or

required to disclose a SAR-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce to the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

AML Record Keeping

SAR-SF Maintenance and Confidentiality

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. We will share information with our clearing broker about suspicious transactions in order to determine when a SAR-SF should be filed. As mentioned earlier, we may share with the clearing broker a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

Responsibility for AML Records and SAR Filing

Our AML Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that SARs are filed as required. We will maintain AML records and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record keeping requirements.

Training Programs

If required by law, we will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

Approval & Signatures

Supervisor Approval

Approve the firm's AML program by signing below.
I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Supervisor Name:	Christopher Hewig, CFA, CFP®
	6/8/18
Supervisor Signature	**Date**

AML Compliance Officer Approval

Approve the firm's AML program and agree to enforce it by signing below.
I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. I am assuming full responsibility for the firm's AML program. I am qualified by experience, knowledge and training. I understand the duties listed under the program and will fulfill those duties.

AML Officer Name:	Christopher Helwig, CFA, CFP®
	6/8/18
Supervisor Signature	**Date**

Anti-Insider Trading Policy

Background

An investment adviser should establish, maintain and enforce written policies and procedures reasonably designed, taking into consideration the nature of such investment adviser's business, to prevent the misuse of material, non-public information by such investment adviser or any person associated with such investment adviser. The SEC defines material by saying "Information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision." Information is nonpublic if it has not been disseminated in a manner making it available to investors generally.

Firm Policy

NWM strictly prohibits trading personally or on the behalf of others, directly or indirectly, based on the use of material, non-public or confidential information. NWM additionally prohibits the communicating of material non-public information to others in violation of the law. Employees who are aware of the misuse of material nonpublic information should report such to the Chief Compliance Officer (CCO). This policy applies to all of NWM's employees and associated persons without exception. Please note that SEC's position that the term "material nonpublic information" relates not only to issuers but also to the adviser's securities recommendations and client securities holdings and transactions.

In addition, this firm has instituted procedures as described in its Anti-Insider Trading Policy, as amended from time to time, to prevent the misuse of material nonpublic information.

Compliance Requirements

The CCO is responsible for:

- Ensuring all employees and associated persons sign a statement acknowledging and agreeing to abide by the firm's anti-insider trading policy;
- Maintaining a list for each firm and associated person listing all securities owned;
- Copies of all transaction confirmations or monthly or quarterly securities account statement summaries from each of these persons;
- Reviewing these confirmations and summaries for inappropriate transactions and reporting them to Supervisor for action; and
- Maintaining record of Supervisor reviews and results.

The employee acknowledgement statement and list of securities owned should be provided to the CCO on the date of association and annually thereafter. All other record-keeping requirements should be done on a quarterly basis, no more than 10 days after the end of the calendar quarter. Reviews of this policy are to be conducted by the CCO on an annual basis at a minimum.

Record-Keeping Policy

Responsibility for Records

The firm's Chief Compliance Officer (CCO) is responsible for keeping all of the firm's records. These records include at a minimum:

- **Code of Ethics Records:** See the Code of Ethics Section of this Manual
- **Privacy Policy Records:** See the Privacy Policy Section of this Manual
- **AML Records:** See the AML Section of this Manual
- **Anti-insider Trading Records:** See the Anti-Insider Trading Section of this Manual
- **Client Account Records Including Transaction Records:** Client folders, when possible, should be kept in alphabetical order with the files inside those folders kept in chronological order. Any time the firm does anything regarding a client's account, there must be some record of the action. All documents relating to a client must be in accordance with policies and procedures.
- **Client Complaint Records:** See the Compliant Policy Section of this Manual
- **Error File:** Any errors the firm makes (trading, for example) must be documented along with the resolution of the error.
- **Form ADV and Brochure Records:** The firm's CCO must retain copies of the current and all previous brochures and brochure supplements.
- **Form ADV Distribution Records:** The firm's CCO must keep a record of providing all new clients the ADV Form 2 brochures. This is recorded in the client contract. The firm's CCO must keep record of the annual distribution, if required, to all existing clients of the most recent ADV or brochure.
- **Advertising Records:** Any time the firm runs an advertisement, sends a newsletter, publishes an article, or does anything that could be considered to be an advertisement, promotion, or marketing campaign, the firm's CCO must keep a copy of it and a record of to whom it was sent. (Note: most states require documents that at sent to 2 or more individuals be maintained, the SEC requires documents that are sent to 10 or more to be maintained.)
- **Soft-Dollar Arrangement Records:** See the Soft-Dollar Section of this Manual, all records relating to soft dollar arrangement will be kept in compliance with policies and procedures.
- **Financial Bookkeeping Records:** The firm's CCO, or designated principal, must monitor the firm's financial books and records and assure that the responsible party is maintaining the required documents and records and that they are current and up to date.

Record Retention Requirements

The firm's CCO shall ensure that all records are kept readily accessible for at least two years and kept at least five years either on-site or at alternative location.

Remote Office Supervision

(For the purpose of this section a remote office is an office location containing IAR(s) or an RIA, regardless of distance from the adviser's main office (which is the location where the Chief Compliance Officer (CCO) is located and the majority of supervisory activities is conducted) that is not visited at least monthly by the adviser's CCO or other designated supervisory principal of the firm.)

NWM understands that the remote office locations present their own unique compliance challenges and has implemented the following additional "remote office" compliance policies and procedures:

1. All remote office personnel will be required to submit all new client account applications and applicable paperwork to the adviser's CCO or other designated personnel for review and submission to the custodian or other appropriate entity.
2. All remote offices will be required to submit for approval all advertising and correspondence material prior to using or sending these items to their clients. This includes items such as, but not limited to; letterhead, business cards, seminars, websites, flyers, brochures, power point presentations, radio and print advertising, etc.
3. Submission and preapproval for the usage of any d/b/a name used by any person or firm located at a remote office location.
4. Since e-mails are considered correspondence, all remote office IARs will be required to use a pre-approved e-mail address that will be monitored by the firm's CCO or designated supervisor.
5. All remote offices are required to immediately report to the CCO or other designated supervisory personnel any and all customer complaints – both verbal and written. This will be followed by further communication including a detailed explanation of the matter from the involved representative.
6. Since the adviser's main office is required to maintain books and records for the firm, copies of all "hard copy" items must be submitted to the main office in a timely manner. An example of a hard copy item would include, but is not limited to; any client applications or other client paperwork done on paper rather than electronically, etc. (Most hard copy items should be scanned and submitted via e-mail attachment or via file upload whenever possible.)
7. All IARs and supervised personnel will be required to sign annual attestation statements acknowledging that they have read, understand, and agree to abide by the policies, procedures, and ethical business standards of the adviser; additionally, remote office supervised personnel may be required to sign a more robust statement with additional items unique to remote office locations.
8. The adviser recognizes that supervising remote personnel and their transactions is a difficult task. Therefore, the adviser requires all remote IARs to keep extensive and complete notes of all client based conversations and transactions. Adviser and remote

personnel should use a joint CRM program or system that will allow the CCO or designated supervisory personnel to remotely review these notes and verify the details surrounding any client activity or transactions. These notes must be readily available for review by the CCO or other designated supervisory personnel.

9. Adviser and remote office personnel will discuss and pre-approve a listing of securities offerings; asset allocation models; and/or investment strategies that remote office IARs are allowed to discuss with their clients.
10. Adviser will conduct periodic reviews of remote office client files (maintained by the adviser's main office) to verify that they are complete and that portfolio holdings are suitable and appropriate for the client's investment profile information in the file. (This may be done additionally, concurrently, or separately from the client file review done at the adviser's main office.)
11. Adviser and remote office personnel agree to schedule in-office reviews, both announced and un-announced on a periodic basis (no less often than bi-annually) that will be dictated by the adviser's CCO or designated supervisory personnel and based on the remote office's activity level, business model, or other items. These reviews will be conducted by the adviser's CCO, other designated supervisory personnel, or a third party compliance consulting firm chosen by the adviser.

Business Continuity Plan

Background

While it is recognized it is not possible to create a plan to handle every possible eventuality, it is the intent of this firm to set up a framework to be used in most likely of scenarios. It is also the intent that this framework provide guidance as to how to respond should an unforeseen situation occur.

Business Description

NWM conducts business managing portfolios and creating financial plans for individuals, businesses and other clients. We do not hold customer funds or securities. NWM does not accept or enter trades.

Emergency Information

Firm Contact Persons

Our firm's two emergency contact persons are:

Cliff Schmardel, (908) 433-7063, cfish851@gmail.com

and

Aurora Helwig, (201) 705-8943, aurorahelwig@gmail.com

Support Services

In the event of an emergency, the following is a list of support services and the methods by which they may be contacted:

Emergency Services (EMS): 911
Fire Department: 911
Police Department: 911

Firm Attorney	
Firm Accountant	
Firm Computer Technician	

This information will be updated in the event of a material change, and our Chief Compliance Officer (CCO) will review the plan on an annual basis.

Firm Policy

Our firm's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the firm's books and records, and allowing our clients to transact business.

Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building or the death of a key member of the firm. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption.

Approval and Execution Authority

Christopher Helwig, CFA, CFP®, a supervisory person, is responsible for approving the plan and for conducting the required annual review. The CCO has the authority to execute this BCP.

Plan Location and Access

Our firm will maintain copies of its BCP and annual reviews, and all changes that have been made to it. A physical copy of the BCP will be stored with the company's Written Policies and Procedures Manual, which is kept at the main office on the bottom drawer of the filing cabinet. An electronic copy of our plan is located in the firm documents section of the CRM software and on www.newportwealth management.com in the firm documents section.

Office Locations

Our office addresses and phone numbers are:

26 Birch Lane Eatontown, NJ 07724
(732) 741-1200

Alternative Physical Location(s) of Employees

In the event of an SBD that makes it impossible or impractical to use any or all of the company offices, we will move our staff from affected offices to the closest of our unaffected office locations.

If none of our other office locations is available, we will move the firm operations to:

125 Half Mile Road, Suite 200, Red Bank, New Jersey, 07701
The telephone number is (732) 741-1200.

An additional alternate location is:

Clients' Access to Funds and Securities

Our firm does not maintain custody of clients' funds or securities, which would be maintained at clients' brokerage firms. In the event of an internal or external SBD, clients' access to funds would not be interrupted.

Data Back-Up and Recovery (Hard Copy and Electronic)

Our firm maintains its primary hard copy books and records and its electronic records at:
26 Birch Lane Eatontown, New Jersey 07701

Christopher Helwig, CFA, CFP® is responsible for the maintenance of these books and records.

The firm backs up its electronic records using cloud based CRM software through Advyzon, yHLsoft, Inc.. Additional client data is stored and backed up through the custodian where client accounts are held.

In the event of an internal or external SBD that causes the loss of our paper records, we will physically recover them from our back-up site. If our primary site is inoperable, we will continue operations from our back-up site or an alternate location. For the loss of electronic records, we will either physically recover the storage media or electronically recover data from our back-up site, or, if our primary site is inoperable, continue operations from our back-up site or an alternate location.

Operational Assessments

Operational Risk

In the event of an SBD, we will immediately identify what means will permit us to communicate with our clients, employees, critical business constituents, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options we will employ will include our Web site, telephone voice mail, secure e-mail, etc. In addition, we will retrieve our key activity records as described in the section above, Data Back-Up and Recovery (Hard Copy and Electronic).

Mission Critical Systems

Our firm's "mission critical systems" are those that ensure client communication, access to client accounts and trading systems. More specifically, these systems include the office computer systems.

We have primary responsibility for establishing and maintaining our business relationships with our clients.

Alternate Communications with Clients, Employees, and Regulators

Clients

We now communicate with our clients using the telephone, e-mail, our Web site, fax, U.S. mail, and in person visits at our firm or at the other's location. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by e-mail but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail.

Employees

We now communicate with our employees using the telephone, e-mail, and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party.

Regulators

We communicate with our regulators using the telephone, e-mail, fax, U.S. mail, and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party.

Regulatory Reporting

Our firm is subject to regulation by the state of New Jersey. We now file reports with our regulators using the IARD/CRD System. In the event of an SBD, we will check with the SEC and/or other relevant regulators to determine which means of filing are still available to us, and use the means closest in speed and form (written or oral) to our previous filing method. In the event that we cannot contact our regulators, we will continue to file required reports using the communication means available to us.

Regulatory Contact:

Death of Key Personnel

The following personnel are identified as "Key Personnel" without which it would be difficult or impossible to continue operating the firm and/or properly service clients:

Christopher Helwig, CFA, CFP®, Day-to-day operations.
If some event made it impossible for any person listed above able to continue to service the firm, the firm would implement the following:

Clients of the firm would be able to obtain the services from another advisor of the firm or would have the choice terminating their agreement and obtaining similar services at another firm.

Updates and Annual Review

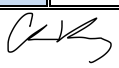
Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our brokerage firm. In addition, our firm will review this BCP annually, to modify it for any changes in our operations, structure, business, or location or those of our brokerage firm.

Approval & Signature

Supervisor Approval

Approve the firm's Business Continuity Plan (BCP) program by signing below.
I have approved this Business Continuity Plan as reasonably designed to enable our firm to meet its obligations to clients in the event of a Significant Business Disruption.

Signed:

Officer Name and Title:	Christopher Helwig, CFA, CFP®
	6/8/18
Supervisor Signature	**Date**