**Full Firm Name**

Policy and Procedures Regarding Information Security

**Revised May 2012**

# Introduction

The Firm (*Name here*) has developed and implemented this information security program (the “Program”), taking into account the manner in which it operates its business, as well as any limitations on the scope of that business, including [DESCRIBE].

1. Are there any additional limitations that should be explained?

The Program complements the Firm’s [privacy] policy and the Firm’s Business Continuity Plan (the “BCP”), including in relation to the Firm’s remediation efforts in response to a cyber-attack or similar incident.

1. Does the firm have a privacy policy?
2. Does the firm have a Business Continuity Plan?

The Program also takes into consideration the Firm’s obligations (a) as an investment Firm registered with the U.S. Securities and Exchange Commission (SEC),

1. Is firm registered with the SEC?

[IF APPLICABLE: (b) as a commodity pool operator and commodity trading Firm registered with the NFA,] and (c) if any, under the laws of the U.S. states in which its clients are resident.

1. Does either (b) or (c) below apply?

The Firm modeled the requirements of the Program relating to the use of its technology on relevant process standards published by [REFERENCE THE APPLICABLE STANDARD (E.G., NIST, ISO).

1. Does the firm use any compliance standard for its security program? (i.e. PCI, NIST, ISO, etc)?

# PII Processing

[ ] (the “Firm”), as part of conducting its business in the ordinary course, obtains and uses personal information of [clients] (“Personal Information”).

1. Does your firm process personal information?
2. What does your firm consider personal information?

Personal Information may be transmitted and retained in technology maintained by the Firm,

1. Is the PII stored on firm equipment?
2. If so, on-site, off-site, or both? (back-up devices should be included)

or licensed by the Firm from third-party vendors (each, a “Vendor,” and collectively, “Vendors”), ~~such as [DESCRIBE],~~ who provide services on an outsourced basis to the Firm [and / or the funds and accounts managed by the Firm (collectively, the “Funds”)].

1. If by third-party/vendors (hereafter known as 3RD-P),
	1. Is there a contract/SLA with the company?
	2. Is the company name kept on file with firm?

The Firm acknowledges that it faces the risk of a cyber-attack on such technology by which a third-party could unlawfully gain access to and misappropriate Personal Information of clients. The threat of this type of third-party misconduct requires that the Firm identify and analyze the material risks to its business created by the use of such technology.

1. If by 3RD-P, does the firm have a process in reviewing the security of these entities?

# Governance

The Firm has designated the [Chief Operating Officer (“COO”)][Chief Technology Officer (“CTO”)][Information Security Governance Committee][OTHER] as the primary point of responsibility for coordinating the firm’s efforts to develop and implement the Program.

1. Has the firm designated someone to carry out its governance?
2. Is so, what is the title of the person?

In carrying out the elements of his or her role in relation to the requirements of this Program, the [COO][CTO][Information Security Governance Committee][OTHER] will be assisted by the [Chief Compliance Officer][Director of Operations][OTHER].

1. Has the firm designated an alternate or assistant to help the designee?

These employees will meet no less than once per quarter with the [Chief Executive Officer][Information Security Governance Committee][OTHER] to review the status of the controls and processes that the Firm has introduced to identify and mitigate cyber-risks, as well as any reports produced in response to periodic assessments of the Firm’s cybersecurity program.

1. How often will the firm meet to assess the security controls (from the compliance standard) or risk mitigations implemented, to ensure they are operating as intended?

# Risk Assessment

Before implementing the Firm’s cybersecurity program, the [COO][CTO][Information Security Governance Committee][OTHER] supervised the completion of a risk assessment (the “Risk Assessment”) commercially reasonably designed to identify foreseeable internal and external risks to the security, confidentiality, and integrity of Personal Information and the systems used by the Firm and critical third-parties to process that Personal Information, where such risks could result in the unauthorized disclosure, misuse, alteration, or destruction of that information or those systems.

1. Has the firm perform a risk assessment?

\*note: the UMA security assessment being performed is different than a risk assessment.

In particular, the Risk Assessment included a review of [LIST RELEVANT PROPRIETARY AND THIRD-PARTY SYSTEMS].

1. If risk assessment performed, what was reviewed? Where third-party tools included in the review?

The focus of the Risk Assessment was on prioritizing the Firm’s systems, and those of its primary vendors, used to conduct [IDENTIFY CRITICAL FUNCTIONS], and evaluating the effectiveness of the controls implemented by the Firm to mitigate these risks, as well as identifying weaknesses and vulnerabilities in the firm’s existing cybersecurity risk controls.

1. If risk assessment performed, what was the focus?
2. What processes do 3RD-P tools support?

The Risk Assessment, and the results obtained by completing that assessment, are][is] in writing.

1. If risk assessment performed, is final report in writing? And accessible?

# Internal Systems

The Firm has developed and implemented the following safeguards intended reasonably to mitigate the risks identified in the Risk Assessment.

**\*Note: even no risk assessment was performed, it is a good idea to have the following in place.**

1. The Firm has implemented technology (directly or through Vendors), including [DESCRIBE], that is capable of being used securely. The Firm maintains a written list of the technology that it utilizes, including technology provided by Vendors to which the Firm [has][and / or the Funds have] outsourced processing and related functions.
2. Is there a vendor list maintained?
3. The Firm monitors the use of technology it utilizes, and the scope of that monitoring is designed to identify any interruptions in the use of such technology. In particular, the Firm’s monitoring processes include the following: [DESCRIBE AND REFERENCE WHO PERFORMS THE MONITORING].
4. Does monitoring of vendor technology
5. The Firm has selected and implemented an appropriate encryption standard [relating to communications][storage of data containing Personal Information]. Specifically, the Firm [DESCRIBE ENCRYPTION STANDARD(S)].
6. What encryption standards are used for PII stored data?
7. What encryption technique, or tool, is used for encrypted email communication?
8. The Firm has established access controls to its network(s), including by [DESCRIBE ACCESS CONTROLS]. In addition, the Firm has confirmed in writing with each of the relevant Vendors that the Vendors maintain access controls to prevent unauthorized representatives of the Firm from accessing any network that contains data relating to the Firm’s business (including Personal Information). [Each relevant Vendor has further warranted to the Firm that it monitors those components of its networks relating to the Firm’s business for unauthorized access to, or service interruptions affecting, such networks.]
9. What access tools or techniques are implemented for network access?
10. What access tools or techniques are implemented for remote access? (i.e. LogMeIn)
11. In regards to vendor access,
	1. In the contract/SLA with the vendor, does it speak to the vendors access controls implemented to protect the firm?
	2. Does the vendor monitor its network at the access points to the firm’s network, or where it may have access to firm information?
12. The Firm has created a written authentication process to enroll and verify any authorized user(s) of technology provided by the Firm. The authentication process is supervised by [IDENTIFY], and consists of [DESCRIBE PROCESS].
13. Does the firm use authentication services or a vendor for access to the network?
14. Does the firm use authentication services or a vendor for remote access? (i.e. LogMeIn)
15. The Firm, with respect to technology that it maintains at its office, continuously monitors its technology and networks for indications of an intrusion. This monitoring is supervised by [IDENTIFY] and consists of [DESCRIBE PROCESS]. Additionally, the Firm has reviewed the monitoring processes employed by each of the relevant Vendors, with respect to technology-based processes outsourced to the Vendor(s) by the Firm [and / or the Funds], and intends to regularly seek updates from the relevant Vendors regarding any material changes in their respective monitoring processes.
16. The firm monitors its network continuously?
17. If it is monitored by a third party, are the monitoring alerts or reports provided to the firm?

# Maintenance of the Program

The Firm evaluates the Program based on the following:

1. Those matters identified as material risks in the Risk Assessment;
2. Relevant changes in technology and business processes, if any;
3. Any material changes in or to the Firm’s operations or business arrangements, including any material change in technology or technology-based services provided by a Vendor; and
4. Any other circumstance that the Firm reasonably believes may have a material impact on the Program.
5. Why does the firm evaluate the program (security\cyber)? \*reference list above.
6. How often is the program evaluated?

In addition, the Firm will not implement a material enhancement to the technology it utilizes (regardless of whether it is maintained by the Firm or by a Vendor) to conduct its principal business until and unless the Firm determines that the enhancement will not result in unreasonable risk of creating a weakness in the Program.

# Vendors

The Firm has taken the following actions intended to identify potential weaknesses and vulnerabilities in the Program as a result of the Firm’s reliance on technology-based processes maintained by Vendors:

1. The Firm has evaluated existing safeguards which restrict access by Firm employees and third-parties to technology provided by Vendors;
2. Does the firm perform #(a) above?
3. If not, will it be implemented?
4. Before the Firm selects a Vendor, it reviews the prospective Vendor’s information security protocols and protections relative to the Firm’s due diligence standards;
5. Does the firm perform #(b) above?
6. If not, will it be implemented?
7. The Firm requires that each Vendor agree in a contract to implement and maintain appropriate safeguards and measures (e.g., [IDENTIFY EXAMPLES) intended to safeguard against the misappropriation of Personal Information; and
8. Does the firm perform #(c) above?
9. If not, will it be implemented?
10. [The Firm monitors Vendors for indications of any security lapses or interruptions relating to networks and data maintained by those Vendors.]
11. Does the firm perform #(d) above?
12. If not, will it be implemented?

**Note: no matter how little vendors are involved, it is a good idea to have some vendor management process to ensure the vendors used do protect the firm’s PII.**

# Consulting Resources

The Firm has identified [and retained] relevant third-party forensic, legal, and other experts capable of assisting the Firm to identify means to enhance those elements of the Program intended to prevent, detect, and remediate attempts by third-parties to penetrate the systems utilized by the Firm (including systems maintained by one or more Vendors).

1. For incident response purposes,
	1. Has the firm identified a third-party forensic provider?
	2. Has the firm have outside counsel on retainer? Or, identified a legal consultant?

# Testing

[No less than once per calendar year][Once per calendar quarter], the Firm will conduct (or will arrange for a third-party to conduct on the Firm’s behalf) a test of the Program intended to identify any vulnerabilities in the processes by which the Firm, or any Vendor, safeguards access to Personal Information against unlawful penetration and misappropriation. In addition, at least once every two (2) calendar years, the Firm will retain a third-party to conduct the test referenced above. In each case, the test will include an assessment of the effectiveness of:

1. How often will the firm perform a security test? (i.e security control review, security assessment, penetration test, security audits, etc).
2. Will the firm perform these, or will a vendor?
3. The Firm’s and each relevant Vendor’s controls relating to access to Personal Information;
4. The encryption technology and / or processes utilized by the Firm and / or each Vendor applicable to the storage and communication of Personal Information;
5. The controls employed by the Firm and each relevant Vendor to detect, prevent, and respond to incidents of unauthorized access to or use of Personal Information; and
6. Employee training provided by the Firm (or any third-party retained by the Firm) relating to the Program.
7. What will the firm what tested for the security test?

\*Please see list above and change based on firm’s needs. Note: it is good to have a compliance standard to follow, this way the firm could test the security controls from that standard (the security controls they chose to fit their needs).

[The assessment referenced above may be completed through, among other things, receiving and reviewing a written summary prepared by each Vendor of internal testing conducted by that Vendor of its own systems.] [Each of the tests referenced above, and the results of each such test, will be summarized in writing.]

1. Will the security test report be provided in writing?

# Training

No less than [once][twice] per year, the Firm (or a third-party retained by the Firm) will train relevant staff regarding the primary elements of the Program. The training will cover, at a minimum, the Firm’s legal and regulatory obligations to protect Personal Information, and a summary of the elements of the Program intended to safeguard such Personal Information, including [DESCRIBE].

1. Does the firm provide this training?
2. Does the training include those items listed above (highlighted in green), or is there additional items?

# Incident Response

The Firm has implemented the following procedures for responding to an incident involving unauthorized access to, or unauthorized disclosure or use of, Personal Information:

1. Does the firm have an incident response plan, especially for breach of PII & required reporting?
2. If no, is there a vendor that handles this?
3. The [COO][CTO][Information Security Governance Committee][OTHER] will direct the assessment of the nature and scope of any such incident, including the circumstances which led to the detection of the intrusion, and will identify the systems, networks, and data involved in the incident;
4. Who is the incident response lead and/or team, as well as their roles? Or the POC that will handle coordination with an outside vendor?
5. On the basis of the [COO’s][CTO’s][Information Security Governance Committee’s][OTHER’s] assessment, the [COO][CTO][Information Security Governance Committee][OTHER] will direct and supervise the actions taken by the Firm to contain and control the incident to prevent further unauthorized access to, or unauthorized disclosure or use of, Personal Information;
6. For incident response RE PII, is a process in place to contain further PII spillage if it should occur?
7. The [COO][CTO][Information Security Governance Committee][OTHER] will conduct (or direct and supervise) a prompt investigation of the incident, with the objective of determining the likelihood that Personal Information has been or will be misappropriated; and
8. Who will lead or conduct the investigation? (like above, who is the incident response team).
9. If the Firm’s assessment indicates that Personal Information has been misappropriated or is reasonably possible, then as soon as possible the [COO][CTO][Information Security Governance Committee][OTHER] will prepare a written summary of what took place and a description of the possible risk(s) of a future breach of the Firm’s system and networks (or the systems and / or networks used by the Firm but maintained by one or more Vendors), in each case to the extent of the Firm’s understanding of the incident, and will provide the written summary to (i) the SEC, [IF APPLICABLE (ii) the CFTC,] and (iii) relevant law enforcement authorities.
10. Who will provide the official written report to the SEC? (like above, who is the incident response team).

The Firm will provide the written summary referred to in (d) above to each client or other individual whose information was misappropriated (or may be misappropriated), unless the regulator and / or law enforcement authorities receiving a copy of the summary request in writing that the notification be delayed. Any notification referenced in (d) will be prepared in compliance with [IDENTIFY RELEVANT STATE BREACH NOTIFICATION LAW, IF ANY], and any other applicable laws and regulations, including the applicable laws and regulations of the jurisdiction in which the affected client(s) reside.

1. Who will provide the official written report to clients that are affected by a PII breach? (like above, who is the incident response team).

The [COO][CTO][Information Security Governance Committee][OTHER] will document the Firm’s actions taken in response to each incident, including any assessment of the nature of what occurred, how the Firm responded to the incident, the scope of any misappropriation of Personal Information, whether the incident will trigger implementation of any processes under the BCP, and the action(s), if any, the Firm intends to take to prevent any future incident.

1. Does the firm maintain after action reports for each incident?

# [11. Insurance [IF RELEVANT]]

[The Firm has purchased information security insurance coverage. The coverage would apply in the event of an information security incident (as referenced in Section 10 above), and is intended to defray the costs incurred by the Firm, among other things, to:

1. Restore network security;
2. Investigate the incident;
3. Recover data believed to be lost as a result of the incident;
4. Obtain legal advice regarding the Firm’s obligations arising from the incident;
5. Respond to any business interruption resulting from the incident;
6. Notify clients regarding the incident; and
7. Respond to any claim brought by a regulator or client, including (with respect to the latter) any claim of breach of privacy.]
8. Does the firm carry insurance?
9. If yes, does the above list #(a)-(g) apply?
10. If not, is there a statement on file to support the management decision?