CYBERSECURITY QUESTIONNAIRE

Thank you for downloading this template. If you have any questions, please give us a call at 770-462-2118.

Visit www.myrialawyer.com for more helpful templates and information.

TEMPLATE
[Insert Company Name]
Cybersecurity Questionnaire

The following questionnaire was prepared to assist the Adviser in its consideration of applicable cyber risks and development of appropriate safeguards and controls designed to reduce such risks (a "Cybersecurity Program"). The questions raised herein are based on guidelines and practices regarding the protection of business and customer records and information against cyber risks discussed in (i) the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*[1]; (ii) the Commodity Futures Trading Commission's *Staff Advisory No. 14-21*[2]; and (iii) the Securities Industry and Financial Markets Association's *Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Business*[3]. This questionnaire is not intended to suggest that the Adviser is required to maintain particular cybersecurity policies and procedures; as with other types of organizations, an investment adviser may be vulnerable to unique risks and possess different risk tolerances and response resources.

Program Administration

- Has the Adviser designated a specific employee to be responsible for overseeing overall privacy and security management and/or developing and implementing security controls?

- Is a specific employee responsible for designating, as appropriate, members of management or the Adviser's personnel to coordinate, implement and regularly assess the effectiveness of the Cybersecurity Program?

- Has the Adviser established cybersecurity roles and responsibilities for members of management, personnel, clients and service providers?

Risk Identification

- Has the Adviser identified the data, personnel, devices, systems and facilities that enable the Adviser to achieve its business purposes?

- Has the Adviser identified reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information and processing systems that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information or systems (collectively, "Security Risks")?

- Has the Adviser established processes and controls to assess, mitigate and safeguard such Security Risks?

- Does the Adviser have a process for addressing any newly identified vulnerabilities?

Safeguards and Controls

<u>Passwords and Encryption</u>

[1] Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[2] Available at http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

[3] Available at http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/.

- Does the Adviser require its systems, software and mobile devices to be password-protected?
- Does the Adviser maintain password security standards (*e.g.*, requiring a minimum number of characters, upper and lowercase letters, etc.) and/or utilize multi-factor authentication processes?
- Does the Adviser require that passwords be changed regularly?
- Does the Adviser use encryption to protect data "at rest" (*e.g.*, files on computers and storage devices) and data in transit (*e.g.*, data being transferred through the Internet)?

Access

- Does the Adviser restrict access to systems and data through preventative and detective controls?
- Has the Adviser established credentials for persons authorized to access:
    - Physical assets (*e.g.*, office equipment, desktop computers and other physical property);
    - Mobile devices; and
    - Software?
- Does the Adviser maintain and test systems access permissions?
- Does the Adviser maintain and test policies regarding its physical operating environments?
- Does the Adviser monitor personnel activity to detect potential Security Risk events?
- Does the Adviser maintain and enforce a data destruction policy?

Software

- Does the Adviser permit only trusted software to be executed on its operating systems?
- Does the Adviser regularly update its anti-virus and web security software?
- Does the Adviser utilize automatic software updates and spot-check that updates are applied?
- Does the Adviser utilize software designed to monitor networks to detect potential cybersecurity events?

Back-Up and Recovery

- Does the Adviser maintain “cloud” or physical external hard-drive backup systems?
- Are the Adviser’s information back-up systems tested periodically?

Monitoring

- Does the Adviser monitor external service providers to detect potential cybersecurity events?
- Does the Adviser monitor its connections, devices, software, and environment for unauthorized access and use?
- Does the Adviser perform vulnerability scans?

Program Testing

- Does the Adviser regularly test or otherwise monitor its Security Risk safeguards, controls, and systems?
- Does the Adviser maintain a written record of the effectiveness of its Security Risk controls, including the effectiveness of, as applicable:
    - access controls on personal information;
    - encryption of electronic information in storage and transit;
    - controls to detect, prevent and respond to incidents of unauthorized access to or use of personal information; and
    - employee training and supervision relating to the Cybersecurity Program?
- Does the Adviser currently, or intend to, arrange for an independent party to test the Cybersecurity Program?

Service Providers

- To the extent that third-party service providers have access to customer records and information, does the Adviser:
    - oversee service providers;
    - take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards; and/or
    - contractually require service providers to implement and maintain appropriate safeguards?

Detection and Response

- Does the Adviser have a process or a system designed to detect malicious code and unauthorized mobile code?
- Are the Adviser's detection processes tested and improved as appropriate?
- Does the Adviser maintain procedures for communicating event detection to appropriate parties, including individuals whose information has been, or may be, compromised?
- Does the Adviser have procedures for:

- assessing the nature and scope of a potential incident involving unauthorized access, disclosure or use of personal information;
- seeking to contain, control and mitigate the incident;
- conducting a reasonable investigation;
- determining the likelihood that personal information has or will be misused; and/or
- maintaining a written record of systems and information involved and steps are taken to address the incident?

- Are notifications from any detection systems investigated?
- Does the Adviser analyze detected events to understand attack targets and methods?

Program Assessment

- Does the Adviser regularly evaluate and adjust the Cybersecurity Program in light of:
  - the results of a risk assessment process;
  - relevant changes in technology and business processes; and/or
  - any material changes to the Adviser's operations or business arrangements?
- Does the Adviser annually assess the Cybersecurity Program, including with respect to its effectiveness?

Personnel and Training

- Has the Adviser trained members of management and personnel as to how to implement applicable aspects of the Program?
- Does the Adviser update its training and re-train managers and personnel as appropriate?
- Are members of the Adviser's personnel advised of their roles and order of operations when a response is needed?

PROPOSED SAMPLE REPORT

_____, 2018

The Cybersecurity Designee conducted a review of the potential cyber risks to which the Adviser may be subject, safeguards in place to guard against such risks and potential changes or supplements to these safeguards. As part of this review, which covered the [_____] period ended [_____], the Cybersecurity Designee:

1. Communicated with the following individuals:

[_____]

[_____]

[_____]

2. Took the following steps and identified and assessed the following safeguards with respect to, among other things, the Adviser's information systems, physical equipment and environment, employee training and risk detection and response procedures (such safeguards, "Cybersecurity Program"):

[_____]

[_____]

[_____]

3. Reported on the annual review and recommended to management of the Adviser the following changes to its Cybersecurity Program during a meeting held on _____, 2018:

[_____]

[_____]

[_____]

4. Addressed the recommended changes summarized above by taking the following steps:

[_____]

[_____]

[_____]