

## SAMPLE INFORMATION SECURITY AND BUSINESS CONTINUITY

### Due Diligence Questionnaire

#### **Background**

As a registered investment adviser, we are required by the U.S. Securities and Exchange Commission and/or the Federal Trade Commission to conduct due diligence on the administrative, technical and physical information security safeguards implemented and maintained by our third-party service providers. This Information Security and Business Continuity Questionnaire is intended to help us assess your ability to (i) insure the security and confidentiality of our records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of those records; and (iii) protect against unauthorized access to or use of those records or information.

We are also required to inquire about your Business Continuity/Disaster Recovery Plan so that we may assess your (i) preparedness for responding to and recovering from an unexpected event and (ii) ability to provide us with uninterrupted services in the event of a disaster or prolonged interruption to the normal course of your business.

#### **Instructions**

The majority of questions require only a "Yes" or "No" response, however, you are encouraged to expand or clarify any response as needed directly after each section in the "Clarifying or Additional Comments" area. Please reference particular question to which you are responding. For any questions deemed non-applicable to your company or if the answer is "None," please respond accordingly (e.g., "N/A" or "None"). Please do not leave blank responses.

#### **Attestation**

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.		
<b>Company Name</b>	<b>Company Address</b>	
<b>Officer's Name and Title</b>	<b>Officer's Signature</b>	<b>Date Signed</b>

**PART I – PRIVACY**

YES	NO	#	QUESTION
		1.	Do you have written privacy policies and procedures?
		2.	Do you have a privacy policy notice that you provide to your customers?
		3.	If so, please provide a copy of the privacy notice.
		4.	Do you have policies and procedures for the proper disposal of customer information?
		5.	Are employees, subcontractors and temporary workers with access to customer data, bound by confidentiality and/or non-disclosure agreements (whether separately or as part of their code of conduct)?
		6.	Where sub-contractors are utilized to provide services to your customers and are provided access to customer data, do you review, or have an independent auditor assess the sub-contractor's security posture?
		7.	Is a formal process in place to address changes to, or new issuance of, privacy laws/regulations and regulatory guidance?
		8.	Do your privacy policies and procedures incorporate employee training?

**Clarifying or Additional Comments (attach additional pages if necessary):**

## PART II – INFORMATION SECURITY

YES	NO	#	QUESTION
		1.	Do you have written policies, procedures and/or guidelines for securing, maintaining and monitoring the security of customer information?
		2.	Are your written information security policies and procedures approved by your senior management and/or your Board of Directors?
		3.	Do your written information security policies and procedures include a risk assessment?
		4.	Does the scope of your risk assessment include an enterprise-wide analysis of internal and external threats and vulnerabilities to confidential customer information?
		5.	Does the scope of your risk assessment include an enterprise-wide analysis of the likelihood and impact of identified threats and vulnerabilities?
		6.	Does the scope of your risk assessment include an enterprise-wide analysis of the sufficiency of policies, procedures and customer information systems to control risks?
		7.	Are your written information security policies and procedures reviewed at least annually?
		8.	Do you have an individual designated to oversee your information security program?
		9.	If yes, in the space provided below, please provide that person's name, title and contact information.
		10.	Do you employ access controls on information systems that contain customer information?
		11.	Do you have a physical security program which defines and restricts access to customer information as well as protects against destruction, loss or damage of customer information?
		12.	Do you store paper records in a room, cabinet, or other container that is locked when unattended?
		13.	Do you ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods?
		14.	Do you encrypt customer information?
		15.	Do you support e-mail encryption (SMTP/TLS or other)?
		16.	Do you use strong passwords (at least eight characters)?
		17.	Do you require the periodic changing of passwords?
		18.	Does your information security program incorporate dual control procedures, and segregation of duties and employee background checks for employees with responsibilities for, or access to, customer information?
		19.	Do you conduct background checks (that include credit, criminal, drug and employment checks) for all consultants, temporary workers and external providers?
		20.	Do you have a formal intrusion detection program for monitoring host and/or network activity?
		21.	Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to customer information?
		22.	If yes, does the plan include customer notification procedures?
		23.	Do you have an employee "acceptable" use policy?
		24.	Do you have an employee security awareness training program?
		25.	If yes, in the space provided below, please indicate how often employees must attest to the policy contents.
		26.	Do you monitor for unauthorized network connection points such as wireless access points, modems etc.?

YES	NO	#	QUESTION
		27.	Do you perform periodic penetration tests on its internet facing network and systems?
		28.	Do you have a process to identify and remedy security vulnerabilities and threats relating to internet facing applications and servers as the threats become known?
		29.	Do you patch critical vulnerabilities on internet facing servers and applications within 4 weeks of the patch becoming available?
		30.	Do you have spyware protection installed on all Windows servers and workstations?
		31.	Do you restrict administrative access to desktops, laptops and PDAs to employees and third parties?
		32.	Do you mandate hard disk encryption for laptops?
		33.	Has a web vulnerability assessment been carried out for applications with connectivity to the internet?
		34.	If backups are stored offsite, are they transported by authorized couriers in protected vehicles and stored in protected and professional storage facilities?
		35.	Are offsite backups containing customer data encrypted?
		36.	Do you have a defined computer incident/data breach policy in place?
		37.	Do you prevent access to removable media such as floppy drives, writeable CDs and DVDs and USB storage devices?
		38.	Are the office facilities and data centers used in providing services to customers guarded?
		39.	Are entry and exit points to office facilities and data centers covered by video surveillance?
		40.	Do you have any of the following certifications? <ul style="list-style-type: none"> <li>• SAS 70 Report</li> <li>• ISO-9000/1 certification</li> <li>• BS 7799 certification</li> <li>• TruSecure</li> <li>• PCI certification</li> <li>• Systrust certification</li> <li>• Webtrust certification</li> <li>• CMMI Certification</li> </ul>
		41.	Does your vendor management program address due diligence, contract provisions, financial condition, risk assessment, ongoing monitoring requirements and third-party relationships such as sub-contractors?

**Clarifying or Additional Comments (attach additional pages if necessary):**

**PART III – DISASTER RECOVERY AND BUSINESS CONTINUITY**

YES	NO	#	QUESTION
		1.	Do you have an organization-wide disaster recovery and business continuity program?
		2.	If yes, in the space provided below, please provide the name of your plan coordinator.
		3.	If yes, please provide a copy of your current disaster recovery and business continuity plans.
		4.	Are disaster recovery and business continuity plans based upon a business impact analysis?
		5.	If yes, do the plans identify recovery and processing priorities?
		6.	Do you have formal agreements for the use of an alternate location should the need arise to relocate operations?
		7.	Do disaster recovery business continuity plans address procedures and priorities for returning to permanent and normal operations?
		8.	Do you maintain offsite backups of critical information?
		9.	Do you have procedures for testing backup media at an offsite location?
		10.	Have disaster recovery and business continuity plans been tested?
		11.	If yes, in the space provided below, list how many employees participate in the test and how often the test is conducted.
		12.	If yes, in the space provided below, please provide the date the plans were tested and a brief summary of the results of any such test.
		13.	If you have experienced a disaster recovery situation in the last 2 years, in the space provided below, please provide details and the procedures invoked

**Clarifying or Additional Comments (attach additional pages if necessary):**