Cyber Security Policy

Overview

BDFSC Holdings Corp. and affiliates ("the Firm") is dedicated to the ongoing protection of client and firm proprietary information whether owned or managed by the Firm, its registered representatives and financial advisors ("advisors"), third-party vendors or financial institutions. As such, the Firm has adopted and implemented this Cyber Security Policy ("CSP") to document its activities to prevent, detect and address cyber security threats or incidents. Through its CSP, the Firm outlines the manner in which it:

- Controls against cyber security threats;
- Identifies potential cyber security threats;
- Responds to suspected or confirmed cyber security incidents; and
- Reviews its cyber security practices to identify weaknesses in its CSP.

These activities, taken together, represent a holistic CSP that is specifically designed to protect the Firm's clients, prospective clients, advisors, associated persons, and related proprietary information.

Scope

The CSP applies to all financial products and services offered and provided by the Firm, and it covers all aspects of the Firm's business activities and client dealings. As such, all individuals associated with the Firm, including its advisors, associated persons, contractors, and consultants, are expected to comply with the requirements outlined herein.

Oversight, Approval and Review

Michael Harken, the Firm's CTO, is responsible for overseeing the CSP and is responsible for its contents and the activities it describes. Additionally, Mr. Harken is responsible for ensuring that

advisors and associated persons comply with its contents. While Mr. Harken is responsible for the CSP, various operational activities and the oversight of them may be delegated in whole or in part by Mr. Harken.

The CSP shall be reviewed and approved at least annually the Firm's executive committee. The annual review and subsequent approval are evidenced the CSP owner's approval of this document in **Appendix A**. Out of cycle reviews by the Firm's executive committee may be warranted due to material changes to the operating or control environment, changes to regulatory requirements, audit findings, or policy exceptions.

CSP

Organizations of all types are becoming more vulnerable to cyber threats due to their increasing reliance on computers, networks, programs and applications, social media, and data. Security breaches can negatively impact organizations and their clients, both financially and reputationally.

Cyber security refers to the technologies, processes, and practices designed to protect an organization's information assets — computers, networks, programs, and data — from unauthorized access. With the frequency and severity of cyberattacks on the rise, there is a significant need for improved cyber security risk management.

It is the policy of the Firm to ensure that cyber security risks are appropriately mitigated against to help protect the security of information and assets owned or managed by the Firm. This CSP outlines the steps that the Firm takes to prevent, detect, and respond to cyber security risks and incidents.

Due to the complexities of managing cyber risk and the countless number of ways that an incident may occur, this CSP may not address all actions taken to address cyber risk. In the event that this policy does not cover a particular topic, reasonable safeguards should be used to protect client and Firm information (e.g., never leaving a computer unattended, never click on links in suspicious emails, do not download programs if you do not know the developer, etc.).

Definitions

Some of the terms used throughout this document are defined below.

Term	Definition
Client information	Client information is inclusive of data specific to each client (e.g., name, address, social security number, etc.) and any information unique to them that may assist the Firm offer its products and services. Client information also includes customer assets or records of them.
Firm information	Firm information is inclusive of information, tools, and other items that assist BDFSC Holdings Corp., its Advisors, and its Associated Persons offer its products and services to clients or prospective clients. Firm information also includes forms, Advisors lists and information, and client lists and information.
Advisors	Advisors and their staff members that conduct securities related business for the benefit of clients or prospective clients.
Associated Persons	Associated persons are individuals who may or may not be employed by the Firm to conduct its ongoing activities, including the execution of the processes outlined by this CSP.
Incident	Any instance, or suspected instance, of a cyber security breach. Incidents can include hacking, denial of service attacks, data leakage, lost or stolen technological assets, and phishing, among others.

Cyber security Risk Management

The Firm employs various preventative and detective controls to mitigate against cyber security threats, which are discussed below. While many of these controls are industry standards, all of them have been tailored to the Firm to ensure that its overall control environment specifically addresses the risks to its clients and firm information. These controls are primarily targeted toward the protection of data, as the Firm recognizes that cyber threats would likely be targeted toward the systems or processes that store or capture sensitive data: data centers, internal networks, externally hosted environments, and business continuity programs. Such data can be stored internally, externally, or both.

The Firm conducts a comprehensive assessment of its cyber security risk management activities at least annually in an effort to identify weaknesses in its control environment that should be addressed. The assessment, which is documented separately in the *CS Risk Assessment*, includes the various information systems, storage locations, third parties, and associated persons that may store, or have access to, client information or firm proprietary information.

Preventative Controls

Preventative controls provide a valuable layer of security over client information and firm proprietary information. Several key preventative controls utilized by the Firm include:

Training

The Firm trains its Advisors and Associated Persons at least annually on cyber security related matters. The intent of which is to ensure that each individual understands their obligations under the CSP. CSP training may be combined, in whole or in part, with other training delivered by the Firm.

Cyber security training includes the following:

- Outline the basic steps that Associated Persons must take to protect client and firm information, which include requirements to:
    - Secure all files, notes, and correspondence with a password
    - Change passwords periodically
    - Never share or display passwords in the open
    - Recognize attempts to obtain client or firm information
- Inform Associated Persons of the activities to be taken in the event of a cyber security incident or a suspected incident

Network Security

The Firm's network has been securely configured, is restricted through access controls which blocks unauthorized access, uses a firewall. Patches and frequent updates are performed to ensure that the network security protocols remain current to guard against leaks or vulnerabilities.

Advisors, contractors, and consultants are expected to employ similar safeguards in the event that their network used to access client or firm information is not directly managed by the Firm.

Protection

To supplement the network security protocols, the Firm also takes steps to ensure that its technology assets are protected against intruders. Some of the controls used include:

- Utilizing current Antivirus software and Spyware
- Ensuring that servers and computers receive updates and security patches

- Using secure configurations for hardware and software on laptops, desktops and servers

Data Security and Access Control

The Firm utilizes various data protection controls to protect data when it is in use, in transit, and while at rest. While not all of the activities taken to protect data are included below, the following key controls are in place to secure data:

- Maintaining an *Asset Inventory Log* of items that use, store, or access data, which includes technology devices and related software (e.g., servers, back-ups, portals, programs, etc.)
- Utilizing least-privilege access controls (i.e., administrator vs. user roles)
- Enforcing standard access control protocols
    - Forced password reset periods
    - Minimum expectations for passwords
    - Disabling accounts after extended periods of not being used
- Utilizing processes for approving and reviewing user access
- Encrypting data at rest or in transit
    - Password protect data stored in programs, network drives, or on disc
    - Protect data sent electronically through the use of secure mechanisms to transfer data (e.g., SFTP, encrypting sensitive information in email, NetDocuments, etc.)

Even if the most technologically advanced cyber security controls are utilized, a company's network and data can easily become compromised if certain physical safeguards are not utilized. The Firm, its Advisors, and Associated Persons:

- Restrict access to servers and connected devices
    - Doors should remain locked at all times
    - Idle computers should be locked
- Passwords should never be written down or left in a location that is easily accessible to unauthorized users
- Documents or media that contain client or firm information are either shredded or erased prior to being discarded

The Firm also recognizes that personal computing devices may be used to connect to secured networks or to access, transmit, or store client and/or firm information. As such, the Firm has

outlined certain requirements in **Appendix B** that should be met when utilizing personal computing devices.

Additionally, should an incident occur that compromises the integrity or completeness of data, appropriate actions will be taken to recover the information as outlined by the *Business Continuity Plan*.

Detective Controls

The Firm employs various detective controls to identify potential breaches of its cyber security defenses, which include:

Monitoring and Testing

The CSP owner has implemented the following activities to identify if an incident has already occurred or vulnerabilities due to weak or preventative controls:

- Quarterly penetration testing
- Quarterly vulnerability scans
- Annual access reviews
- Conducting reviews of Advisors and third-parties, as described below
- Continuous scanning devices and software for malware

Any concerns identified as a result of these reviews will be logged on an *Incident Report* and addressed accordingly. Some of these activities may be conducted in conjunction with the annual refresh of the CS Risk Assessment.

Review

Continued compliance with, and effectiveness of, the CSP is assessed through various reviews conducted by the Firm or a qualified third-party. The reviews can be conducted either individually or collectively. At a minimum, the activities outlined by this CSP should be reviewed at least annually. The review may be conducted in conjunction with the annual refresh of the *CS Risk Assessment*. The actions taken to perform the review and any substantive findings shall be documented and submitted to the CSP owner. The report can be combined with other annual reports used to report on the effectiveness of the Firm controls.

Advisors

The Firm relies upon the activities of independent advisors to offer its products and services to clients or prospective clients. The use of independent advisors poses unique threats to an entity primarily because they are asked to develop, maintain and use their own networks, systems, and security protocols. To help cope with these risks, advisors are required to comply with the CSP, which will be documented, in part, through an annual attestation using the *CS Attestation – Advisors* (**see Appendix C**).

To help guard against the introduction of cyber threats through the use of advisors, the Firm:

- Ensures that advisors' contracts contain provisions specific to managing cyber risks, including:
    - Requirements to comply with all the Firm policies and procedures, which includes this CSP
    - Right to audit clause
    - Expectations on minimum cyber security requirements for the networks and systems under their control
    - Requirement to report known cyber security incidents impacting the Firm
- Requires that advisors receive cyber security training
- Requires that advisors implement certain of the preventative and detective controls highlighted in this CSP. More specifically, network security, data security and access controls, and asset protection protocols for both digital and physical assets if the Firm resources are not utilized.

<u>Oversight of Advisors</u>

The CSP owner conducts or delegates to the appropriate party the following activities for Advisors:

- Reviews Advisors in line with the branch review audits that includes cyber security components
- Requires that each advisor complete the *CS Attestation – Advisor* annually.
- Obtains and reviews completed *CS Questionnaire for Advisors*

Third-Party Vendors, Consultants, and Contractors

The Firm utilizes various third-party vendors, consultants, and contracted agents to manage client assets and to perform other administrative functions including custody, clearing, trading, compliance, and filing.

To help guard against the introduction of cyber threats from a third-party, the Firm:

- Ensures contracts contain provisions specific to managing cyber risks, including:
    - Requirement to supply service organization control (SOC) reports, if available
    - Right to audit clause
    - Expectations on minimum cyber security requirements
    - Requirement to report known cyber security incidents impacting the Firm

Oversight of Third-Party Vendors, Consultants, and Contractors

The CSP owner conducts or delegates to the appropriate party the following activities, at least annually, for third-party vendors, consultants, and contractors:

- Obtains and reviews SOC reports, if available
- Reviews access to networks, applications, and other portals used to access third-party tools and programs
- Assesses the need for cyber security audits and conduct them where warranted
- Obtains and reviews completed *CS Questionnaire for Independent Contractors and Consultants*

Incident Reporting and Response

Cyber security attacks are perpetuated for varied reasons including, but not limited to: financial fraud, information theft or misuse, activist causes, to render computer systems inoperable, and to disrupt critical infrastructure and vital services of a government or organization. They can be executed through outright attacks of a network or be part of elaborate schemes involving social engineering, including phishing emails and malicious phone calls.

Incidents identified shall be immediately reported to the CSP owner who will keep a log that includes certain information related to the incident and corrective actions taken. When practical, an *Incident Report* should be utilized to capture the pertinent details of the incident for record-

keeping purposes; however, receipt of the form is not required nor is it needed in order to appropriately respond to the incident.

Upon notification, the CSP owner will assess the reported incident and take necessary steps to address the incident. The actions taken to address incidents will vary. In some cases, a detailed action plan detailing the implementation of new preventative or detective may be required while no action may be needed in others.

Regulatory Obligations

The following regulatory obligations are addressed by the CSP. It is important to note that this is not an exhaustive list, as guidance and case law may not be included below:

Agency	Citation	Title
SEC	Regulation S-P	Requires written policies and procedures to protect client information against cyber-attacks and other forms of unauthorized access
SEC	Regulation S-ID	Outlines firm's duties regarding the detection, prevention, and mitigation of ID theft
FINRA	Rule 3110	Requires firms to implement effective oversight

Table 1: Cyber security Regulatory Obligations

Exceptions

Exceptions to the CSP are expected to be infrequent but may be warranted to address specific business needs. Exceptions must be approved, in writing, by the CSP owner and must be documented. The exception documentation must capture the rationale for the exception, an assessment of risk associated with the exception (if appropriate), expiration dates for the exception (if applicable), and any other relevant information. All exceptions will be periodically reviewed to assess their ongoing necessity.

Appendix A: Document Review and Approval Log

Version	Date	**Change(s) Made**	**Approver**
1.0	July 31, 2017	Initial policy development	Lisa Smith Michael Harken Barb Bennett Robert Sherwood
1.1	August 24, 2017	Changes made from Board Acknowledgement	Lisa Smith Michael Harken Barb Bennett Robert Sherwood

Appendix B: Personal Computing Devices

The use of personal computing devices (e.g., smart phones, tablets, etc.) introduce unique cyber security risks to the Firm, its Advisors, any Associated Persons, and its clients or prospective clients. Such risks are inherent to the portability of personal computing devices ("Devices") and their functionality as a stand-alone computer. That said, the following minimum safeguards must be followed to ensure that cyber security risks are mitigated should a device that is used to conduct firm-related activities be lost or its security compromised:

Security

- Passwords or other authentication methods must be used to access Devices
- Devices must be set to automatically lock after a period of inactivity
- Users must have the ability to remotely wipe Devices
- Users must notify CSP owner if a Device is lost or stolen within 48 hours or as soon as practical after the incident has occurred

Network

- Devices should only be connected to known, secure networks
- Limit use of unknown or unsecure networks
    - Known, secure networks include those that are password protected and controlled by the Firm or an Associated Person
    - Note: The use of cellular or Wi-Fi networks made available by your cellular provider is acceptable.

Software

- Users should take reasonable steps to ensure that the most current operating system is installed on Devices
- Third-party software used to access client-related information through the device (e.g., trading platforms, etc.) must be:
    - Secured through additional authentication measures separate from the Device access protocol
    - The most current version offered by the provider

Appendix C: CS Annual Attestation – Advisor

As an Advisor of BDFS Holdings Corp. and affiliates ("the Firm"), I understand that I am required to comply with the Cyber Security Policy ("CSP"). I also understand that I am obligated to ensure that all individuals associated with my relationship with the Firm comply with the CSP, which includes administrative assistants and other support staff.

In line with the expectations included in the CSP, I specifically attest that:

___ My network is securely configured, is restricted through access controls which blocks unauthorized access, and uses a firewall;

___ My technology assets (e.g., computers, servers, etc.) use current Antivirus software and Spyware, receive updates and security patches as soon as they are available, and use secure configurations;

___ My office and I utilize the various data protection controls outlined in the Data Security and Asset Control section to protect data when it is in use, in transit, and while at rest, which includes requirements on the use of Personal Computing Devices; and

___ I will immediately escalate any cyber security incident or suspected incident to Michael Harken or Robert Sherwood.

Please initial each item and sign below.

Financial Advisor	
Signature	
Date	