

INFORMATION SECURITY POLICIES AND PROCEDURES

Adopted Effective February 1, 2019

Overview:

Senior management takes seriously the need to adhere to best practices concerning the protection of confidential information. ThinkBetter, LLC (“ThinkBetter” or “Firm”) has taken steps to protect the information it has obtained related to its business and its clients. The Information Security Policies and Procedures are a critical function of the Firm’s business operations.

As part of its assessment of the needs related to such Policies and Procedures, and taking into account the manner in which it operates its business, ThinkBetter has developed and implemented this information security program (the “Program”), which outlines technical and administrative controls to prevent, detect, and correct risk.

1. Introduction

Maintaining the trust of our clients is a key to our success. Because ThinkBetter may possess confidential information about our business and portfolios, as well as personal information about our clients (“Personal Information”), ThinkBetter has implemented the following policies and procedures.

Personal Information and other confidential information may be transmitted and retained in technology or systems maintained by ThinkBetter, or it may be provided by ThinkBetter to third-party vendors (each, a “Vendor,” and collectively, “Vendors”). ThinkBetter acknowledges that its technology faces the threat of a cyber-attack, by which an outside party could unlawfully gain access to Personal Information and other confidential information. In order to mitigate this threat and enhance its information security policies, ThinkBetter seeks to identify and analyze the material risks to its business associated with the use of such technology.

Unless granted an exception by the Chief Information Security Officer (CISO) or designee, all ThinkBetter employees must abide by the policies set forth in this document. If the CISO is not available, a designee will fulfill the responsibilities in his/her place. Failure to comply with ThinkBetter policies and procedures may lead to disciplinary action, including termination.

The Program complements ThinkBetter’s client Privacy Policy and ThinkBetter’s Business Continuity Plan (the “BCP”), in relation to ThinkBetter’s remediation efforts in response to a cyber-attack or related incident. The Program also takes into consideration ThinkBetter’s obligations as an investment adviser registered with the US Securities and Exchange Commission, and under the laws of the States in which its clients reside, as applicable.

2. Governance

ThinkBetter has designated that the Chief Information Security Officer (CISO) has the primary responsibility for coordinating the firm’s efforts to develop and implement the Program. The CISO may confer with the CCO or a designee in the development and implementation of the Program. The CISO reports to Senior

Management with regard to the oversight of the Program and may coordinate with the Chief Executive Officer, Chief Compliance Officer (“CCO”) and/or their designees.

3. Risk Assessment

On at least an annual basis, ThinkBetter will complete an information security risk assessment (“Risk Assessment”) to ensure that its senior management is aware of any risks or vulnerabilities and takes appropriate actions to remediate the risk.

ThinkBetter categorizes risk broadly to include people, processes, and technology. The Risk Assessment is designed to identify foreseeable internal and external risks to the security and confidentiality of Personal Information and the systems used by ThinkBetter’s critical third parties including, but not limited to, vendors that process information where such risks could result in the unauthorized disclosure, misuse, alteration, or destruction of that information or those systems. ThinkBetter’s review considers various threats that may have an impact on its assets, including business changes, increased volume, and threats that are malicious, natural, or accidental. The Risk Assessment aims to evaluate the effectiveness of existing cybersecurity risk controls and identify any weaknesses; it also places special focus on the systems maintained by ThinkBetter and its primary vendors that process and retain client information.

The Risk Assessment and its results will be maintained in writing and reviewed by the CISO or a designee to determine if any additional controls are necessary. The results of the assessment are confidential, and access is limited to specified key individuals.

4. Access Controls

Employees are given access to certain ThinkBetter’s systems only upon completion of the new hire process, which includes a thorough background check. ThinkBetter seeks to limit access to confidential client information and other proprietary firm information to those employees who require access to such information in order to complete their job duties and responsibilities. ThinkBetter does not disclose, and no Employee may disclose, any Personal Information about a client or former client other than in accordance with the procedures stated herein and in the Employee Code of Conduct and the Policies and Procedures Manual (“Compliance Manual”).

Physical Access:

Upon employment, ThinkBetter will grant its employees access to the building and its common areas. Access to the server room is not allowed without authorization by the CISO or a designee. Additionally, hard copies of confidential records are maintained in locked filing cabinets.

The Building is secure at all times, and employees must use a security badge or key to enter the building.

System Access:

ThinkBetter maintains its information systems, including hardware, software, and network design components in order to protect and preserve Personal Information. All computers with access to ThinkBetter’s information must have anti-virus/malware detection software with current definitions.

Employees use passwords for computer access, as well as for access to specific programs and files. Passwords shall be changed if there is reason to believe they have been compromised. Network passwords are automatically reset every one hundred and eighty (180) days.

Firewalls and encrypted transmission have been set up to maintain security and confidentiality when ThinkBetter’s network is accessed remotely by authorized persons.

Electronic media, such as computers, laptops or cellular devices, on which Non-Public Personal Information is stored, shall be formatted and restored to initial settings prior to any sale, donation, or transfer of such equipment.

ThinkBetter does not allow clients to access its internal systems. Any client information is shared via a secure connection or authorized third-party content sharing tools. ThinkBetter's policy regarding emails containing confidential client information should be encrypted and should have the smallest possible distribution given the purpose of the communication. Any request to use content sharing tools must be approved by the CISO or a designee.

Employee Termination:

The CISO or a designee must be notified prior to the termination of any employee. Upon the resignation of an employee, ThinkBetter will conduct a review of that employee's current projects, roles, and responsibilities to determine the risk associated with continued access for the duration of employment. Based on that risk, interim measures may be taken to further limit access to client and firm confidential information.

If the termination is involuntary, ThinkBetter will immediately revoke all systems and physical access as part of its termination procedures. Termination of access to systems will be documented by the CISO or a designee.

Access Review:

On at least an annual basis, ThinkBetter will conduct a review of the access policies and procedures described above. This process will audit system security and projects to ensure that security is appropriate. The review will be conducted by the CISO, or their designee, and documented and maintained as part of ThinkBetter's books and records. Any items found to be a breach of policy or confidentiality will be reviewed by the CCO or designee and appropriate action will be taken.

5. Maintenance of the Program

ThinkBetter evaluates the Program based on the following:

- Those matters identified as material risks in the Risk Assessment
- Relevant changes in technology and business processes
- Any material changes to ThinkBetter's operations or business arrangements, including any material change in technology or technology-based services provided by a Vendor
- Any other circumstance that ThinkBetter reasonably believes might have a material impact on the Program

In addition, ThinkBetter will not implement a material enhancement to the technology it utilizes unless approved by the CISO or designee.

6. Vendor Due Diligence

In connection with the Risk Assessment, ThinkBetter will conduct due diligence on Vendors to identify potential weaknesses and vulnerabilities in the Program. Vendor due diligence will focus on areas that are identified as higher risk or that pose material risks to the safety of Personal Information and other confidential information. Vendor due diligence may include:

- Evaluation of existing safeguards to restrict access by ThinkBetter employees and third parties to technology provided by Vendors

- Review of prospective Vendor's information security protocols and protections relative to ThinkBetter's due diligence standards and according to the Vendor's roles and responsibilities
- Monitoring Vendors for indications of any security lapses or interruptions relating to networks and data maintained by those Vendors

Furthermore, ThinkBetter will require each Vendor to agree in a contract to implement and maintain appropriate safeguards against the misappropriation of Personal Information.

ThinkBetter may use initial and/or annual due diligence questionnaires to assist in evaluating Vendor's controls related to the storage and communication of Personal Information. Additionally, ThinkBetter may request policies and procedures and/or internal/external audit reports of Vendors related to the detection, prevention, and response to incidents of unauthorized access to or use of Personal Information.

Vendor due diligence as described above will be maintained as part of ThinkBetter's books and records.

7. Testing

ThinkBetter will conduct ongoing testing (or will arrange for a third party to conduct testing on ThinkBetter's behalf) of the Program to identify any vulnerabilities in the processes by which ThinkBetter safeguards access to Personal Information. To the extent practical and reasonable, the testing may include a review of:

- ThinkBetter's controls relating to access to Personal Information
- The encryption technology and/or processes utilized by ThinkBetter applicable to the storage and communication of Personal Information
- The controls employed by ThinkBetter to detect, prevent, and respond to incidents of unauthorized access to or use of Personal Information
- Employee training provided by ThinkBetter (or a third party retained by ThinkBetter) relating to the Program

Testing and reviews of the Program will be maintained as part of ThinkBetter's books and records.

9. Training

No less than annually, ThinkBetter (or a third party retained by ThinkBetter) will train relevant staff to adhere to the 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.

10. Incident Response

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

1. The CISO or designee will direct the assessment of the nature and scope of any such incident. The assessment will consider the circumstances that led to the detection of the intrusion identify the systems, networks, and data involved in the incident
2. On the basis of his assessment, the CISO or designee, in consultation with the CCO or a respective designee, will direct and supervise the actions taken by ThinkBetter to contain and control the incident
3. The CISO and/or CCO or designee will conduct a prompt investigation of the incident to determine the likelihood that Personal Information has been or will be misappropriated

4. If ThinkBetter's assessment indicates that Personal Information has been misappropriated, then the CISO or designee will prepare a written summary of (a) what took place and (b) the potential risk(s) to ThinkBetter's system and networks (or the systems and/or networks used by ThinkBetter but maintained by one or more Vendors), in each case to the extent of ThinkBetter's understanding of the incident. As applicable and given the nature of the incident, the summary may be provided to (i) the Executive Committee, (ii) the SEC or State regulatory agencies, and/or (iii) relevant law enforcement authorities
5. An assessment will be made as to the need to notify any regulatory bodies, including, but not limited to, the Securities and Exchange Commission and state securities regulators

ThinkBetter will also provide the written summary to each client or individual whose information was misappropriated (or could be misappropriated), as required by law unless the regulator and/or law enforcement authorities receiving a copy of the summary request in writing that the notification be delayed. Any notification will be prepared in compliance with the applicable state regulations and any other applicable laws or regulations, including the laws and regulations of the jurisdiction in which the affected client(s) reside.

The CISO and/or CCO or designee will maintain a log ("Incident Response Log"), which will document each incident, including ThinkBetter's assessment of the nature of what occurred, how the incident was resolved, and any further actions taken to prevent such an incident from occurring again.

Any questions concerning the Information Security and Cybersecurity Policies and Procedures may be directed to info@thinkbetter.us

End of Policy