Mark C. Scheffler Senior Portfolio Manager, Founder

Appleton Group - Cybersecurity Policy

Cybersecurity is a critical topic of interest to the investment industry, investment industry regulators and our clients. As such, it is important that together we identify and understand our Company's cybersecurity risks. The risks to our firm associated with cybersecurity include but are not limited to (i) reputation risk; (ii) financial risk; and (iii) regulatory risk. None of these can be taken lightly, which is why evolving our cybersecurity policies and procedures is so important.

Appleton Group's Cybersecurity Program include the following:

1. **Employee Training:** Without proper training, any company's employees and vendors may inadvertently put sensitive data at risk. Some data breaches may result from unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured internet connection, or opening messages or downloading attachments from an unknown source. With proper training, however, employees and vendors can be Appleton Group's first line of defense, such as by alerting the firm's Chief Compliance Officer (CCO) to a suspicious activity and understanding and following our Company's policies and procedures with respect to technology.

    - On an annual basis Appleton Group will conduct a Cybersecurity training program for all Company employees to review the Company's cybersecurity policies and procedure.

2. **Risk Evaluation, Access Controls, and Data Loss Prevention:** Cybersecurity risk assessment processes relative to the key areas of the Company's business are extremely important. Any company may be particularly at risk of a data breach from a failure to implement basic controls to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes. Finally, some data breaches may result from the absence of robust controls in the areas of system configuration.

    - Appleton Group has entered into a service contract with **CMIT Solutions** to provide the Company with cloud based cybersecurity, back-up services, disaster recovery services and business continuity services.

    - On an annual basis the Company will conduct a "Disaster Recovery and Cybersecurity Test" to verify all critical Company and client documentation and information is properly backed up, and secure from system failures, computer viruses, malware, dangerous spyware, and unauthorized client information access.

3. **Vendor Management:** The Company has developed a **Vender Due Diligence Checklist,** which all outside vendors must complete at the time they enter into a contract with Company and annually.

4. **Incident reporting procedures:** Appleton Group acknowledges the increased risks related to cybersecurity attacks, potential future breaches, system failures and data loss.

    - It is the duty of every Company officer, employee and associate to report all potential cybersecurity breach situations to the CCO.

    - It is then the CCO's responsibility to investigate the situation and determine how the situation should be handled. The CCO may need to involve other Company associates, outside vendors, custodians and regulators. A final report must be written by the CCO once the situation has been addressed, resolved and documented.

    - If a cybersecurity policy or procedure needs to be revised it is the responsibility of the CCO to verify that the policy or procedure is revised and implemented.

Adopted: December 8, 2015

Mark C. Scheffler
Managing Member, Chief Compliance Officer