Cybersecurity at Sentinel Benefits

Ensuring data protection for our clients.

Today's world—often referred to as the "information age"—has seen people generate, store and exchange information at an unparalleled rate of frequency and volume. This has greatly changed the ways in which we interact with one another, not just as individuals, but also within and between organizations. Countless benefits have emerged, but these have arrived with serious challenges in the areas of security and privacy, manifested by the growing amount of new regulations concerning the storage of data.

As a leading financial services institution committed to both integrity and innovation, Sentinel Benefits & Financial Group has an ethical, legal and professional obligation to ensure the information we hold follows the principles of confidentiality and accessibility.

We believe effective data security starts with employee awareness, training and risk assessment.

- Information security constitutes a significant investment—from training our people to ensuring the right mix of systems and operational controls are in place to ensure protection.
- Our associates are regularly trained, made aware of security practices and privacy-related regulations, and are required to take an annual security awareness training course. Our software developers are also required to take additional courses related to creating secure application programs.
- Our technology team has implemented its own internal phishing testing and awareness campaign to measure and benchmark employee awareness to suspicious emails. The team also initiates an annual penetration test done by an independent third party ethical hacker.
- Cyber security incident response is one part of our disaster recovery testing in which our associates participate.
- Analyzing risk is a critical first step—from rating and performing due diligence on third party vendors to reviewing safety, privacy and general compliance issues through our Risk Committee, we make risk assessment and mitigation a priority.
- We maintain a number of security-related policies and procedures including a Cyber Security and Incident Response policy (using the SEC's recommended NIST framework) and a Written Information Security Policy.

We invest in technologies that secure our environment.

- We utilize commercial network perimeter security devices to secure our network.
- We continuously deploy software programs that detect attack patterns, respond immediately, and alert IT personnel. These intrusion-detection and prevention solutions are in addition to anti-spam, anti-advertisement and anti-virus solutions.
- We prescribe to alert services such as USCERT the U.S. homeland security email alerts, as well as other sources to monitor developing security threats, trends, and known new weaknesses.
- We complete annual audits and attestations like the SSAE 16 audit that review the accuracy and completeness of data center operations.
- Encryption technologies are utilized to protect data "in flight" and "at rest."
- Remote access capabilities utilized by employees require dual factor authentication to access internal systems.

Visit **https://www.cybersecurity.sentinelgroup.com** if you have additional questions about Sentinel Benefits & Financial Group's approach to cybersecurity, or contact Todd Larson, Chief Information Officer, at (781) 914-1405.

Date of First Use: 1/28/2019

Sentinel Benefits & FINANCIAL GROUP