Inland Securities Corporation
Cybersecurity Policy

Policy

ISC’s cybersecurity policy, in conjunction with our Firm's Identity Theft and Privacy policies recognizes the critical importance of safeguarding clients' personal information as well as the confidential and proprietary information of the firm and its employees. Maintaining the security, integrity and accessibility of the data maintained or conveyed through the Firm's operating systems is a fundamental requisite of our business operations and an important component of our fiduciary duty to our clients. While recognizing that the very nature of cybercrime is constantly evolving, ISC conducts periodic vulnerability assessments based on our firm's use of technology, third-party vendor relationships, reported changes in cybercrime methodologies, and in response to any attempted cyber incident, among other circumstances.

Protecting all the assets of our clients, and safeguarding the proprietary and confidential information the firm and its employees is a fundamental responsibility of every ISC employee, and repeated or serious violations of these policies may result in disciplinary action, including, for example, restricted permissions or prohibitions limiting remote access; restrictions on the use of mobile devices; and/or termination.

Background & Procedure

On March 26, 2014 the SEC sponsored a Cybersecurity Roundtable to develop a better understanding of the growing cybersecurity risks and to facilitate discussions about the ways in which regulators and the industry can work together to address them, according to Commissioner Luis Aguilar, in a speech he presented on April 2, 2014 to the Mutual Fund Directors Forum.

On April 15, 2014, OCIE staff issued an NEP Risk Alert, OCIE Cybersecurity Initiative, "to provide additional information concerning its initiative to assess cybersecurity preparedness in the securities industry."

Recently a cybersecurity taskforce was formed and a third party vendor, Terre Verde was engaged by the Inland Group to perform an assessment for Inland Securities (“ISC")

ISC and Inland Computer Services are currently working together to develop and implement policies and procedures that address cybersecurity gaps identified in the Terre Verde analysis.

Responsibility

ISC’s Compliance Officer will be responsible for reviewing, maintaining and enforcing policies and procedures in order to meet ISC’s overall cybersecurity goals and objectives as well as ensuring compliance with applicable federal and state laws and regulations. ISC’s Compliance Officer may recommend to the firm's board of directors any disciplinary or other action as appropriate. ISC’s Compliance Officer will also be responsible for distributing and training cybersecurity policies and procedures to employees.

Any questions regarding ISC’s cybersecurity policies should be directed to ISC’s Compliance Officer.