The Director will have overall responsibility for a comprehensive security program that includes information security policies, compliance and governance with the expanded scope to include internal employees, external clients and Firm-sponsored audits of third-party suppliers and vendors. This position will be responsible for developing long-term security strategies and ensuring the Firm meets all security standards, regulatory expectations, and the coordination of responses to client audit requests and questionnaires. In addition, this position will provide security-related vision, leadership, and strategy required to succeed with the ever changing market conditions. This position reports to the Chief Information Officer.

RESPONSIBILITIES:

Provide leadership for the integration of security as a key component of the Firm's culture.

Responsible for the planning and development of an enterprise information security strategy and best practices in support of the Firm's information security architecture.

Develop test plans for all phases of unit testing, acceptance testing and acceptance testing and implementation of projects related to information security.

Collaborate with key business and Technology leaders to develop security and business continuance standards and action plans.

Direct the creation of compliance procedures and documentation for internal information security procedures.

Provide oversight of the process to collect and provide evidence for client and Firm questionnaire, audit, and incident investigations.

Understand and anticipate security trends internal and external to the Firm and keep the Firms senior management informed about information security-related issues and activities affecting the Firm.

Proactively communicate to the internal user community to consistently exceed defined levels of security needs.

Communicate key information security strategies and processes to increase productivity and/or to reduce risk.

Provide leadership for defensive technology and processes that include intrusion detection, proactive hunting and analytics, incident handling, vulnerability assessments, and remediation.

Oversee incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary.

Responsible for ensuring that tools or technologies are implemented to reduce the risk of disruptive attacks against systems or threats to confidentiality.

Manage the development, implementation, and regular review of Firm cyber security policies, standards, guidelines and procedures to ensure ongoing maintenance of security.

Develop, deliver and maintain an education and security awareness program on information security and privacy matters for attorneys and staff.

Understand and assess potential threats, vulnerabilities and control techniques and advises the Firm.

QUALIFICATIONS:

Minimum of ten years of progressive experience in computing and information security, including experience with internet technology and security issues within the legal services marketplace.

Minimum of four years as an Information Security Officer or a comparable scope information security role in a medium to large organization.

Four-year college degree preferred in Computer Science, Information Management, comparable experience considered.

Ability to empower and lead a team to meet business and IT security goals.

Demonstrated people management skills providing direction, change leadership, monitoring performance, motivating staff and building a positive working environment.

Ability to adapt to a fast-moving IT landscape and keep pace with latest thinking and newest security technologies.

Desire to drive the IT security strategy forward.

Strong analytical thinker capable of managing numerous information sources and providing data analysis reports to senior management.

Ability to read, analyze and interpret instructions furnished in written, oral, diagram or schedule form.

Ability to meet the demands of internal and external users and clients.

Ability to effectively present information, and work with users at all levels in the Firm.

Ability to change direction where required and showing flexibility to meet new demands.

Ability to make timely and informed decisions.

Ability to look at alternatives and consider new ways of thinking to problem solve.

Ability to manage several concurrent projects and prioritize demands.

Experience maintaining and updating policies and procedures.

Demonstrated experience handling sensitive or confidential information.

Strong communication (oral and written) skills.

Prior experience in legal information technology or information security preferred.

Possession of, or working toward processional certifications such as GIAC credentials, CISM, or CISSP.

Send Resume to:
Paula Kurtzman, Senior Recruiter
pkurtzman@friedmanwilliams.com
1430 Broadway, 9th Floor, New York, NY 10018
Main Line: 212 -867-7000