Owner: CTO
Effective From: October 2015

For Display on Notice Boards

Information Security Policy Statement

Forensic Risk Alliance // Information Technology

For the technology systems and processes, related business activities, and maintenance and management of Internet and Web services and systems related to Data Collections and Forensics, Client Data Processing and Hosting, and Internal Systems having interaction with Production Processing and Hosting systems.

Our Company

FRA is a market leader in regulatory compliance, financial investigations, and data analytics. We specialize in supporting clients facing cross-border litigation, multi-jurisdictional anti-corruption investigations, and civil, regulatory, and criminal financial investigations. We are expert providers of litigation support, forensic accounting services, international eDiscovery, and data forensics solutions.

We support our clients by providing evidence on complex financial issues, advising on anti-corruption measures, performing reviews, testing controls, developing risk assessments, implementing compliance programs, and assuring evidence compliance through data forensics and e-Discovery. In addition, we have developed a unique expertise in addressing data protection across borders by utilizing our data centers in Europe and North America in tandem with portable solutions and on-site hosting.

Our Organization

The organization of and arrangements for information security management are detailed in the FRA Information Security Management System (ISMS).

The Chief Technology Officer is responsible for the overall direction of and commitment to information security, and for authorizing this policy. Information security objectives are established and achieved by the implementation of a set of controls, including policies, practices, procedures, organizational structures and software functions.

The Director of Security and Compliance, supported by the aforementioned CTO, has direct responsibility for maintaining this policy, the ISMS, its associated policies, processes, procedures and standards and providing advice and guidance on their implementation.

Department Directors/Managers are directly responsible for implementing the relevant policies, processes and procedures within their respective departments, and for adherence by their employees.

All persons work for or on behalf of FRA have a duty to comply with the requirements of this policy.

Our Commitments

FRA understands that constant vigilance in information security is critical for both our business as well as the customers that rely on our support, services and solutions. We therefore commit to delivering the high level of service that FRA is known for, while protecting our clients' data from internal, external, deliberate and accidental threats.

In short, we are committed to continual improvement, minimizing risks that could threaten the Confidentiality, Integrity and Availability of all our clients' data, and ensure all legal and regulatory requirements relevant to the jurisdictions in which our clients' data are held are adhered to.

All managers are directly responsible for implementing the Security Policy within their business areas, and for adherence by their staff.

It is the responsibility of each member of staff to adhere to the Security Policy. Failure to do so may result in disciplinary action.

Signed:

Gregory Mason
CTO