# FRA INFORMATION SECURITY POLICY STATEMENT

*The following is the **Information Security Policy Statement** for the family of Forensic Risk Alliance entities (Forensic Risk Alliance, Inc.; Forensic Risk Alliance, Ltd.; Forensic Risk Alliance, SARL; Forensic Risk Alliance, SA; and Forensic Risk Alliance Sweden filial), referred to below as 'we', 'us', and 'our'.*

## Policy

We have implemented an information security management system (ISMS) using the framework and requirements as set forth in the ISO/IEC 27001:2022 standard. The unique needs and objectives, security requirements, organizational processes used, and the size and structure of this organization and those we service influence the establishment and implementation of our ISMS.

It is our policy that all information and data used to conduct FRA business (whether client, employee, or FRA generated business data) is defined as "FRA Information", and it is incumbent upon us to protect it. Specifically, it is our policy that all FRA Information:

- Is properly categorized
- Is protected against unauthorized access or disclosure
- Is protected against unauthorized or inappropriate modification
- Is maintained in a manner that ensures it is available to those persons appropriately authorized

Therefore:

Our Chief Technology Officer (CTO) is responsible for the overall direction of and commitment to information security and for authorizing this policy.

Our Head of Legal and any of their appointed designee(s), are authorized by the CTO and have direct responsibility and authority for maintaining this policy, the ISMS, its associated governance and standards, and for providing advice and guidance on the departmental policies that are governed by these standards.

All individuals dealing with FRA Information, regardless of their status (e.g. employee, contractor, vendor, etc.), must comply with this and all our related policies. All Partners, Directors, and Managers are directly responsible for implementing this policy, as well as designing and implementing related policies within their business areas, and for adherence by their staff.

Finally, as the unique needs, requirements, and indeed even the stakeholders in our program evolve, we must ensure that our program continues to meet and service them. Therefore we are committed to a program that both monitors the performance of and ensures the continuous improvement of our ISMS.

It is the responsibility of each individual to adhere to this and all related FRA Policies. Failure to do so is subject to disciplinary action.

**Gregory Mason, CTO**