Verisk Analytics, Inc. (the “Company”)

Whistleblower Policy – Reporting Concerns Related to Financial Irregularities, Policy Violations, and Ethical Violations
(November 2021)

Introduction

The Audit Committee of the Verisk Analytics Board of Directors has adopted the Whistleblower Policy – Reporting Concerns Related to Financial Irregularities, Policy Violations, and Ethical Violations to establish procedures for the receipt and handling of complaints, including those submitted by employees, as to accounting or auditing matters. This Policy also includes methods for employees and other interested parties to raise concerns with respect to violations of the Company’s Code of Business Conduct and Ethics, other Verisk Policies, and potential violations of laws, rules, or regulations.

Scope

The Policy provides guidance for interested parties, including employees, to raise concerns. While the list below provides examples of the types of subjects covered by this Policy, this list is not intended to be exhaustive, and any person with related concerns should raise those in accordance with this Policy.

• The Company’s accounting, auditing, or internal controls, such as:
  – Fraud or intentional error in the preparation or review of the Company’s financial statements
  – Fraud or intentional error in the audit of the Company’s financial statements
  – Any attempts to mislead or improperly influence the Company’s independent auditor in the course of the performance of its audit
  – Fraud or intentional error in the recording and maintenance of the Company’s financial books and records
  – Deficiencies or noncompliance with the Company’s internal controls
• Public disclosures of the Company’s financial position, such as:
  – Material misrepresentations or omissions regarding the reporting of the Company’s business and financial condition, results of operations, or cash flows, including prospective reports

• Violations of the Company’s Code of Business Conduct and Ethics or other Verisk Policies such as:
  – Improper usage of Company property or funds
  – Improper disclosure of proprietary information
  – Improper use or disclosure of data or information entrusted to our care

• Any act or suspected act of bribery or any act that may be a violation of the Verisk Analytics Anti-Bribery and Corruption Policy

• Concerns regarding employee relations or employee safety and physical security

• Concerns regarding data privacy and/or cybersecurity matters

Non-Retaliation and Confidentiality

Verisk does not tolerate retaliation against anyone who speaks up in good faith to report concerns about behavior that does not follow our Verisk Policy, Code of Business Conduct and Ethics or the law. This includes concerns about any observed, suspected, illegal, unethical behavior, or Code-related Policy violations. Any employee of the Company who raises a good faith concern through these methods should do so without fear of dismissal or retaliation of any kind. Employee submissions will be maintained anonymously where allowed by law. Verisk will maintain confidentiality, in particular the identity of the employee raising the concern, except as may be necessary to conduct a thorough investigation or as required to be disclosed by law or to legal counsel.

Raising a Concern

Concerns related to these matters can be raised to:

• The Office of the General Counsel.

• Internal Audit

• Global Compliance and Privacy Services Department

• The Whistleblower Hotline, 24/7/365, by:
  – Submitting a web-based report on http://verisk.ethicspoint.com/
  – Submitting a telephone report using one of the global hotline phone numbers available by country location

The concerns raised through these channels should include sufficient information and detail to enable the conduct of a thorough investigation. Confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review and legal requirements.
Handling of Concerns

- Any reported concerns shall be communicated to the General Counsel.
- The General Counsel or appropriate designee will acknowledge receipt of the matter to the individual who raised the concern, whenever possible.
- All concerns raised will be reviewed by the appropriate departments with oversight by the Office of the General Counsel:
  - Accounting, auditing, or internal control matters will be reviewed under the direction and oversight of Internal Audit
  - Data Privacy concerns will be reviewed by Global Compliance and Privacy Services
  - Cybersecurity concerns will be reviewed by Enterprise Risk Management
  - Ethical and compliance concerns or violations of Policy will be reviewed by Global Compliance and Privacy Services
  - Employee relations concerns will be reviewed by People Leadership and Culture (HR)
  - Employee Safety and Physical Security concerns will be reviewed by Enterprise Risk Management
- All concerns related to the violations of the Policy, or any other matters raised through these channels, will be reviewed initially by the General Counsel or an appropriate designee in the Law Department, or the Global Compliance and Privacy Services Department.
- After initial review, the General Counsel will determine whether the matter warrants an investigation and will oversee any such investigation. If the matter requires escalation, the General Counsel will discuss at any time the concerns raised with the Audit Committee or the Chair of the Audit Committee. The person(s) authorized to conduct the investigation will report to the General Counsel in a timely manner all findings of fact, conclusions, and proposed recommendations for remedial actions, if any.
- Prompt and appropriate corrective action will be taken when and to the extent warranted in the judgment of the General Counsel in consultation with the Audit Committee.
- The General Counsel will maintain a log of all complaints, tracking their receipt as well as any investigation and resolution, and shall prepare a periodic summary report semiannually for the Audit Committee. Copies of complaints and such log will be maintained in accordance with the Company’s policy regarding document retention.

The Company will not retaliate or discriminate against any employee with respect to the good faith reporting of concerns raised.

The Audit Committee may revise or amend this Policy as necessary or appropriate.